دليل المستخدم

برنامج مكافحة الفيروسات ٢٠٠٩ من KASPERSKY

عزيزي مستخدم برنامج مكافحة الفيروسات 2009 من Kaspersky!

نشكركم لاختيار منتجنا. ونطمح أن تساعدكم هذه الوثيقة في عملكم وتمدكم بإجابات لتساؤلاتكم حول هذا البرنامج.

+٧ (٤٩٥) ٦٤٥-٧٩٣٩،
التليفون والفاكس: +٧ (٤٩٥) ٧٩٧-٨٧٠٠،
+٧ (٤٩٥) ٩٥٦-٧٠٠٠

http://www.kaspersky.com/
http://support.kaspersky.com/

تاريخ المراجعة: ١٣-١١-٢٠٠٨

جدول المحتويات

مقدمة

في هذا القسم:

الحصول على معلومات حول التطبيق

إذا كانت لديك أية تساؤلات تتعلق بشراء أو تثبيت أو استخدام التطبيق، فالإجابات متاحة على الفور.

يتوافر لدى Kaspersky Lab العديد من مصادر المعلومات، والتي يمكنك من خلالها اختيار المصدر الأنسب إليك وفقًا لضرورة وأهمية تساؤلك.

مصادر معلومات البحث الخاص بك

يمكنك استخدام نظام التعليمات.

يحتوي نظام التعليمات على معلومات حول إدارة حماية الكمبيوتر: كيفية عرض حالة الحماية وفحص مختلف المناطق بالكمبيوتر والقيام بمهام أخرى.

لفتح نافذة التعليمات، انقر ارتباط التعليمات في نافذة التطبيق الرئيسية أو اضغط **<F1>**.

الاتصال بإدارة المبيعات

إذا كانت لديك تساؤلات حول اختيار أو شراء التطبيق أو تمديد فترة استخدامه، يمكنك الاتصال بمختصي إدارة المبيعات هاتفياً في مكتبنا الرئيسي بموسكو على الأرقام التالية:

+٧ (٤٩٥) ٧٩٧-٨٧-٠٠ ،+٧ (٤٩٥) ٦٤٥-٧٩-٣٩ ،+٧ (٤٩٥) ٧٠-٠٠

هذه الخدمة متاحة باللغتين الروسية والإنجليزية.

يمكنكم إرسال تساؤلاتكم إلى إدارة المبيعات على عنوان البريد الإلكتروني التالي sales@kaspersky.com.

الاتصال بخدمة الدعم الفني

إذا قمت بشراء التطبيق بالفعل، يمكنك الحصول على معلومات حوله من خدمة الدعم الفني من خلال الهاتف أو عبر الإنترنت.

سيقوم مختصو خدمات الدعم الفني بالإجابة على تساؤلاتكم المتعلقة بتثبيت التطبيق واستخدامه، وإذا كان جهاز الكمبيوتر مصاباً، فسوف يساعدونكم في التخلص من عواقب أنشطة البرمجيات الخبيثة.

طلب بالبريد الإلكتروني إلى خدمة الدعم الفني (خاص للمستخدمين المسجلين فقط)

يمكنك طرح تساؤلك على مختصي خدمة الدعم الفني من خلال ملء نموذج ويب طلب المساعدة (http://support.kaspersky.com/helpdesk.html).

يمكنك كتابة سؤالك باللغات الروسية أو الإنجليزية أو الألمانية أو الفرنسية أو الأسبانية.

لإرسال رسالة بريد إلكتروني تتضمن تساؤلك، يجب إدخال رقم العميل وكلمة المرور التي تحصل عليها أثناء عملية التسجيل بموقع خدمات الدعم الفني.

> ملاحظة
>
> إذا لم تكن مستخدما مسجلا بعد في تطبيقات Kaspersky Lab، يمكنك ملء نموذج تسجيل عبر https://support.kaspersky.com/en/PersonalCabinet/Registration/Form/. سوف يتعين عليك أثناء التسجيل تقديم رمز التفعيل أو اسم ملف المفتاح.

ستقوم خدمة الدعم الفني بالرد على طلبك في الخزانة الشخصية الخاصة بك على الارتباط https://support.kaspersky.com/en/PersonalCabinet، وعلى البريد الإلكتروني الذي حددته في طلبك.

قم بوصف المشكلة التي واجهتك بالتفصيل قدر الإمكان في نموذج الطلب على الويب. حدد المعلومات التالية في الحقول الإلزامية:

- **نوع المطالبة**. يتم تجميع أسئلة المستخدمين الشائعة في موضوعات خاصة، على سبيل المثال "مشكلة تثبيت/إزالة البرنامج" أو "مشكلة فحص/إزالة الفيروس". إذا لم يكن هناك موضوع مناسب لسؤالك، الرجاء تحديد موضوع "أسئلة عامة".

- **اسم التطبيق ورقم الإصدار.**
- **نص المطالبة.** صف المشكلة التي واجهتها بأكبر قدر ممكن من التفصيل.
- **رقم العميل وكلمة المرور.** أدخل رقم العميل وكلمة المرور التي تلقيتها أثناء التسجيل بموقع ويب خدمة الدعم الفني.
- **عنوان البريد الإلكتروني.** ستقوم خدمة الدعم الفني بإرسال الإجابة على سؤالك إلى عنوان البريد الإلكتروني هذا.

الدعم الفني عبر الهاتف

إذا صادفتك أية مشكلة تتطلب مساعدة عاجلة، يمكنك الاتصال بأقرب مكتب للدعم الفني. سوف يلزمك تقديم معلومات تعريف (http://support.kaspersky.com/support/details) عند تقدمك بطلب إلى الدعم الفني من داخل روسيا (http://support.kaspersky.com/support/support_local) أو من خارجها (http://support.kaspersky.com/support/international) Technical Support. فسوف يعمل ذلك على مساعدة المختصين لدينا في معالجة طلبكم في أقرب وقت ممكن.

مناقشة تطبيقات KASPERSKY LAB على منتدى الويب

إذا لم يتطلب تساؤلكم رداً عاجلاً، يمكنكم مناقشته مع مختصي Kaspersky Lab ومع مستخدمين آخرين لبرامج Kaspersky في منتدى الويب الخاص بنا على الارتباط http://forum.kaspersky.com/.

ويمكنكم في هذا المنتدى استعراض الموضوعات الموجودة وترك ردودكم وإنشاء موضوعات جديدة واستخدام محرك البحث.

ما الجديد في برنامج مكافحة الفيروسات 2009 من KASPERSKY

يستخدم برنامج مكافحة الفيروسات 2009 من Kaspersky (والمشار إليه أيضًا بـ "برنامج مكافحة الفيروسات من Kaspersky" أو "التطبيق") أسلوبًا جديدًا تمامًا في حماية البيانات يقوم على أساس تقييد حقوق كل برنامج في الوصول إلى موارد النظام. ويساعد هذا الأسلوب على منع الإجراءات غير المرغوب فيها التي تقوم بها البرامج الخطرة والمشكوك فيها. وقد تمَّ كذلك تحسين قدرة التطبيق على حماية البيانات السرية الخاصة بكل مستخدم إلى حد كبير. ويشتمل التطبيق الآن على معالجات وأدوات تعمل بشكلٍ كبير على تيسير القيام بمهام محددة لحماية الكمبيوتر.

هيا بنا نستعرض الميزات الجديدة لبرنامج مكافحة الفيروسات 2009 من Kaspersky:

ميزات الحماية الجديدة:

- يؤدي فحص نظام التشغيل والبرامج المثبتة لاكتشاف النقاط القابلة للاختراق والتخلص منها إلى الحفاظ على ارتفاع مستوى أمان النظام والحيلولة دون اختراق البرامج الخطرة للنظام الخاص بك.

- تسهل المعالجات الجديدة لمحلل الأمان وتكوين المستعرض إجراء فحص وإزالة تهديدات الأمان ونقاط الاختراق في البرامج المثبتة وكذلك تسهيل تكوين نظام التشغيل والمستعرض.

- تتعامل Kaspersky Lab بصورة أسرع الآن مع التهديدات الجديدة نظراً لاستخدام شبكة اتصال أمان Kaspersky التي تقوم بجمع بيانات حول إصابة أجهزة كمبيوتر المستخدمين وإرسالها إلى خوادم Kaspersky Lab.

- يعمل معالج استعادة النظام الجديد على إصلاح أي ضرر يلحق بنظامك بسبب هجمات البرمجيات الخبيثة.

ميزات حماية جديدة لاستخدام الإنترنت:

- تمَّ تحسين الحماية ضد دخلاء الإنترنت بإدراج عناوين المواقع الاحتيالية في قواعد بيانات التطبيق.

- يتم توفير استخدام آمن للمراسلة الفورية من خلال أداة تقوم بفحص حركة ICQ وMSN.

الميزات الجديدة لواجهة التطبيق:

- تعكس واجهة التطبيق الجديدة المنهج الشامل لحماية المعلومات.

- وتساعد سعة المعلومات العالية لمربعات الحوار المستخدم في اتخاذ قرارات سريعة.

- كما تم التوسع في مجموعة وظائف تسجيل الإحصائيات و إنشاء التقارير. يمكن استخدام عوامل التصفية لتحديد بيانات من التقارير، وهي تعد أداة فعالة ومرنة لا بديل لها عند المحترفين.

نظرة عامة على حماية التطبيق

يقوم برنامج مكافحة الفيروسات من Kaspersky بحماية جهاز الكمبيوتر ضد التهديدات المعروفة وغير المعروفة وكذلك ضد البيانات غير المرغوبة. تتم معالجة كل نوع من التهديدات بواسطة مكون تطبيق مستقل. ويؤدي ذلك إلى مرونة الإعداد وسهولة خيارات التكوين لكافة المكونات والتي يمكن إعدادها وفقًا لاحتياجات مستخدم بعينه أو مؤسسة بأكملها.

يتضمن برنامج مكافحة الفيروسات من Kaspersky الميزات الوقائية التالية:

- مراقبة أنشطة النظام من جانب تطبيقات المستخدم وهو ما يحول دون حدوث أية إجراءات خطرة بواسطة التطبيقات.
- توفر مكونات الحماية حماية في زمن حقيقي لكافة مسارات نقل البيانات والإدخال عبر جهاز الكمبيوتر الخاص بك.
- أمان الإنترنت، يوفر الحماية ضد الهجمات الاحتيالية.
- تستخدم مهام فحص الفيروسات لفحص الملفات أو المجلدات أو الأقراص أو مناطق محددة بمفردها أو فحص الكمبيوتر بأكمله بحثًا عن الفيروسات. يمكن أيضًا تكوين مهام الفحص لاكتشاف النقاط القابلة للاختراق في تطبيقات المستخدم المثبتة.
- يضمن مكون التحديث الإبقاء على تحديث حالة كل من وحدات التطبيق وقواعد البيانات المستخدمة لاكتشاف البرامج الخبيثة وهجمات القراصنة والرسائل غير المرغوب فيها.
- تسهل المعالجات والأدوات تنفيذ المهام التي تتم أثناء عمل برنامج مكافحة الفيروسات من Kaspersky.
- ميزات الدعم التي توفر المعلومات والمساعدة للعمل مع التطبيق وزيادة إمكانياته.

المعالجات والأدوات

يعد ضمان أمان الكمبيوتر مهمةً معقدة تتطلب المعرفة بخصائص نظام التشغيل والطرق المستخدمة لاستغلال نقاط الضعف بهذا النظام. هذا بالإضافة إلى أن حجم وتنوع المعلومات المتعلقة بأمان النظام يجعل من عملية تحليلها ومعالجتها أمرًا صعبًا.

للمساعدة في حل مهام معينة في توفير أمان الكمبيوتر، تمَّ تضمين مجموعة من المعالجات والأدوات في حزمة برنامج مكافحة الفيروسات من Kaspersky.

- معالج محلل الأمان الذي يقوم بتشخيص الكمبيوتر، للبحث عن النقاط القابلة للاختراق في نظام التشغيل وفي البرامج المثبتة على الكمبيوتر.
- يقوم معـــــالج تكـــوين المســـــتعرض بتحليل إعدادات مستعرض Microsoft Internet Explorer لتقييمها من ناحية الأمان في المقام الأول.
- يقوم معالج استعادة النظام بالتخلص من أي تتبعات لهجمات البرمجيات الخبيثة على النظام.

- معالج قرص الإنقاذ الذي يقوم باستعادة مجموعة وظائف النظام بعد التعرض لهجوم فيروسات أدى إلى تلف ملفات نظام التشغيل وتعذر بدء تشغيل جهاز الكمبيوتر.

ميزات الدعم

يشتمل التطبيق على عدد من ميزات الدعم المصممة للإبقاء على تحديث التطبيق وزيادة إمكانياته ومساعدتك في استخدامه.

شبكة اتصال أمان Kaspersky

شبكة اتصال أمان من **Kaspersky** عبارة عن نظام يقوم تلقائيًا بنقل تقارير حول التهديدات المكتشفة والمحتملة إلى قاعدة بيانات Kaspersky Lab المركزية. تتيح قاعدة البيانات هذه إمكانية قيام Kaspersky Lab بالرد على التهديدات الأكثر انتشارًا بشكلٍ أسرع وإخطار المستخدمين عن انتشار الفيروس.

الترخيص

عندما تقوم بشراء برنامج مكافحة الفيروسات من Kaspersky، فإنك بذلك تبرم اتفاقية ترخيص مع Kaspersky Lab والتي تحكم استخدام التطبيق بالإضافة إلى وصولك إلى تحديثات قاعدة بيانات التطبيق وحصولك على الدعم الفني لفترة زمنية محددة. وتتوافر شروط الاستخدام وغيرها من المعلومات اللازمة لعمل مجموعة وظائف التطبيق بالكامل في ملف مفتاح الترخيص.

يمكنك من خلال استخدام وظيفة الترخيص الحصول على معلومات تفصيلية حول الترخيص الحالي أو شراء ترخيص جديد أو تجديد الترخيص الحالي.

الدعم

يمكن لكافة المستخدمين المسجلين لبرنامج مكافحة الفيروسات من Kaspersky الاستفادة من خدمات الدعم الفني الخاصة بنا. للإطلاع على المعلومات المتعلقة بكيفية الحصول على الدعم الفني، الرجاء استخدام وظيفة الدعم.

بإتباعك للارتباطات، يمكنك الوصول إلى منتدى مستخدمي منتج Kaspersky Lab أو إرسال تقارير الخطأ إلى الدعم الفني أو تقديم تعقيبات بشأن التطبيق من خلال إكمال نموذج خاص عبر الإنترنت.

يكون لك أيضًا حق الوصول إلى خزانة المستخدم الشخصية وخدمة الدعم الفني عبر الإنترنت. ويسعد العاملون لدينا دومًا بتقديم الدعم حول التطبيق عبر الهاتف.

التحليل المساعد على الاكتشاف

تستخدم طريقة التحليل المساعد على الاكتشاف في بعض مكونات الحماية التي تعمل في الوقت الحقيقي، مثل مكون مكافحة فيروسات الملفات ومكافحة فيروسات البريد الإلكتروني ومكافحة فيروسات الويب.

تقوم عملية فحص الكائنات باستخدام طريقة التوقيع التي تستخدم قاعدة بيانات تحتوى على وصف لجميع التهديدات المعروفة بتقديم إجابة محددة حول ما إذا كان الكائن الذي تم فحصه خبيثًا أم لا وكذلك الخطأ الذي يمثله. تهدف طريقة التحليل المساعد على الاكتشاف التي تختلف عن طريقة التوقيع إلى اكتشاف السلوك النموذجي للكائنات بدلاً من محتواها الثابت، إلا أنها لا يمكنها تقديم نفس الدرجة من التأكيد في استنتاجاتها.

تكمن ميزة التحليل المساعد على الاكتشاف في أنه يكتشف البرمجيات الخبيثة غير المسجلة في قاعدة البيانات، بحيث لا يلزم عليك تحديث قاعدة البيانات قبل إجراء الفحص. ولهذا السبب، يتم اكتشاف التهديدات الجديدة قبل أن يواجهها محللو الفيروسات.

ومع ذلك فهناك طرق لخداع التحليل المساعد على الاكتشاف. إحدى هذه الإجراءات الدفاعية هي تجميد نشاط الرمز الخبيث بمجرد أن يكتشف الكائن الفحص بطريقة التحليل المساعد على الاكتشاف.

ملاحظة

يضمن استخدام مجموعة من طرق الفحص توفير قدر أكبر من الأمان.

عند فحص كائن ما، يقوم المحلل المساعد على الاكتشاف بمحاكاة تنفيذ الكائن في بيئة افتراضية آمنة يوفرها التطبيق. وفي حالة اكتشاف نشاط مشكوك فيه أثناء تنفيذ الكائن، فسوف يعتبر الكائن خبيثًا ولن يُسمح بتشغيله على المضيف وسوف تظهر رسالة تطلب من المستخدم تقديم تعليمات أخرى:

- عزل الكائن، يتيح فحص التهديد الجديد ومعالجته فيما بعد باستخدام قواعد بيانات محدثة.
- حذف الكائن.
- تخطي (إذا كنت على يقين بعدم كون هذا الكائن خبيثاً).

لاستخدام طرق التحليل المساعد على الاكتشاف، حدد مربع الاختيار استخدام المحلل المساعد على الاكتشاف وحرك شريط تمرير تفاصيل الفحص إلى أحد هذه المواضع: سطحي أو متوسط أو مفصل. يقدم مستوى تفصيل الفحص توازنًا بين شمولية، ومن ثم جودة، الفحص للبحث عن تهديدات جديدة ومدى العبء الواقع على موارد نظام التشغيل، بالإضافة إلى مدة الفحص. وكلما زاد مستوى التحليل المساعد على الاكتشاف، كلما زادت موارد النظام اللازمة للفحص وطالت مدته.

تحذير!

تقوم Kaspersky Lab بالتحليل السريع للتهديدات الجديدة المكتشفة باستخدام طريقة التحليل المساعد على الاكتشاف، ويتم إضافة طرق التنظيف الجديدة إلى تحديثات قاعدة البيانات على مدار الساعة.

إذا قمت بتحديث قواعد بياناتك بانتظام، فسوف تحافظ بذلك على مستوى الحماية الأمثل لجهاز الكمبيوتر على الدوام.

متطلبات النظام من الأجهزة والبرامج

للسماح لجهاز الكمبيوتر أن يعمل بشكلٍ طبيعي، يجب أن يستوفي الكمبيوتر الحد الأدنى من المتطلبات التالية:

متطلبات عامة:

- مساحة خالية بالقرص الثابت قدرها 75 ميجا بايت.
- محرك أقراص صلبة CD-ROM (لتثبيت التطبيق من قرص التثبيت المدمج).
- ماوس.
- برنامج Microsoft Internet Explorer 5.5 أو أحدث (لتحديث قواعد بيانات التطبيق ووحدات البرامج عبر الإنترنت).
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home Edition (SP2 أو أحدث)، *Microsoft Windows XP Professional (SP2* أو أحدث)، *Microsoft Windows XP Professional x64 Edition*:

- معالج Intel Pentium بقدرة 300 ميجا هرتز أو أعلى (أو مكافئ متوافق).
- ذاكرة وصول عشوائي 256 ميجا بايت

Microsoft Windows Vista Home Basic ، *Microsoft Windows Vista Starter x32* ، *Microsoft Windows Vista Business* ، *Microsoft Windows Vista Home Premium* ، *Microsoft Windows Vista Ultimate* ، *Microsoft Windows Vista Enterprise*:

- معالج Intel Pentium بقدرة 800 ميجا هرتز 32 بت (x86) / 64 بت (x64) أو أعلى (أو مكافئ متوافق).
- ذاكرة وصول عشوائي 512 ميجا بايت

تهديدات أمان الكمبيوتر

يمكن أن يتعرض أمان الكمبيوتر للخطر عن طريق تطبيقات التهديد والبريد غير المرغوب والبرامج الاحتيالية وهجمات القراصنة والبرمجيات الإعلانية والشعارات. ويعتبر الإنترنت المصدر الرئيسي للتهديدات.

في هذا القسم:

تطبيقات التهديد

يمكن لبرنامج مكافحة الفيروسات من Kaspersky اكتشاف آلاف من البرمجيات الخبيثة التي قد تستقر في جهازك. تمثل بعض هذه البرامج تهديدًا مستمرًا لجهاز الكمبيوتر، بينما لا يشكل البعض الآخر خطورة إلا في أحوال معينة. بعد اكتشاف التطبيق لأحد التطبيقات الخبيثة، فإنه يقوم بتصنيفه وتعيينه في مستوى خطر (مرتفع أو متوسط).

يقوم محللو فيروسات Kaspersky Lab بتصنيف الفيروسات إلى فئتين رئيسيتين من تطبيقات التهديد: برمجيات خبيثة وبرامج يحتمل كونها غير مرغوب فيها.

برمجيات خبيثة (البرمجيات الخبيثة) (انظر صفحة ١٤) تم إنشاؤها لإلحاق الضرر بالكمبيوتر ومستخدمه: على سبيل المثال، للاستيلاء على معلومات أو منعها أو تعديلها أو مسحها أو تعطيل تشغيل جهاز كمبيوتر أو شبكة اتصال كمبيوتر.

برامج يحتمل كونها غير مرغوب فيها (PUP) (انظر صفحة ٢٦) تختلف عن البرمجيات الخبيثة في أن الغرض منها لا يقتصر على إلحاق الضرر فقط، بل يمكنها المساعدة في اختراق نظام أمان جهاز الكمبيوتر.

تحتوي موسوعة الفيروسات (http://www.viruslist.com/en/viruses/encyclopedia) على وصف مفصل لهذه البرامج.

برمجيات خبيثة

يتم إنشاء البرمجيات الخبيثة ("برمجيات خبيثة") خصيصًا بغرض إلحاق الضرر بأجهزة الكمبيوتر وبمستخدميها: للاستيلاء على معلومات أو منعها أو تعديلها أو إزالتها أو تعطيل تشغيل أجهزة الكمبيوتر أو شبكات اتصال الكمبيوتر.

تنقسم البرمجيات الخبيثة إلى ثلاث فئات فرعية: الفيروسات وفيروسات الدودة وبرامج حصان طروادة وأدوات مساعدة البرمجيات الخبيثة.

الفيروسات وفيروسات الدودة (Viruses_and_Worms) (انظر صفحة١٥) تستطيع إنشاء نسخ من نفسها والتي تنتشر بدورها وتعيد نسخ نفسها مرة أخرى. يتم تشغيل بعض هذه البرامج دون علم المستخدم أو دون مشاركة منه، بينما يتطلب البعض الآخر قيام المستخدم ببعض الإجراءات كي يتم تشغيلها. تنفذ هذه البرامج إجراءاتها الخبيثة عند تنفيذها.

برامج حصان طروادة (Trojan_programs) (انظر صفحة ١٨) لا تشبه الفيروسات وفيروسات الدودة حيث إنها لا تنسخ نفسها. وهي تصيب جهاز الكمبيوتر عن طريق البريد الإلكتروني أو مستعرض ويب على سبيل المثال، وذلك عند زيارة المستخدم لموقع ويب "مصاب". ولابد من بدء تشغيلها بواسطة المستخدم، كما أنها تنفذ إجراءاتها الخبيثة عند تشغيلها.

أدوات مساعدة البرمجيات الخبيثة (Malicious_tools) (انظر صفحة ٢٣) يتم إنشاؤها لإلحاق الضرر على وجه الخصوص. ومع ذلك فإنها على العكس من البرمجيات الخبيثة الأخرى، لا تقوم بأنشطة خبيثة بمجرد تشغيلها ويمكن تخزينها وتشغيلها بأمان على كمبيوتر المستخدم. يتوافر بهذه البرامج وظائف يستخدمها القراصنة في إنشاء فيروسات وفيروسات دودة وبرامج حصان طروادة أو في تنظيم هجمات شبكة اتصال على الخوادم البعيدة أو قرصنة أجهزة كمبيوتر أو القيام بأنشطة خبيثة أخرى.

الفيروسات وفيروسات الدودة

الفئة الفرعية: الفيروسات وفيروسات الدودة (الفيروسات_و_فيروسات الدودة)

مستوى الخطورة: مرتفع

تقوم الفيروسات وفيروسات الدودة التقليدية بإجراءات غير مسموح بها على الكمبيوتر المصاب، من بينها إنشاء نسخ من نفسها وانتشارها.

الفيروس التقليدي

بعد تسلل فيروس تقليدي إلى النظام، فإنه يصيب أحد الملفات ويقوم بتفعيل نفسه وينفذ نشاطه الخبيث، كما يضيف نسخ من نفسه إلى ملفات أخرى.

تقوم الفيروسات التقليدية بنسخ نفسها فقط في الموارد المحلية للكمبيوتر المصاب، إلا أنه يتعذر عليها اختراق أجهزة كمبيوتر أخرى بصفة مستقلة. لا يتم الانتشار داخل أجهزة كمبيوتر أخرى إلا إذا قام الفيروس بإضافة نسخة منه في ملف مخزن داخل مجلد مشترك أو قرص مدمج، أو إذا قام المستخدم بإرسال رسالة بريد إلكتروني تحتوي على مرفقات مصابة.

عادة ما يكون رمز الفيروس التقليدي مخصصًا لاختراق منطقة معينة بجهاز كمبيوتر أو نظام تشغيل أو تطبيق. ووفقاً لبيئة التشغيل، فهناك فرق بين فيروسات الماكرو والملف والتمهيد والبرنامج النصي.

تستطيع الفيروسات إصابة الملفات من خلال استخدام العديد من الطرق. فيروسات الكتابة فوق الملفات تقوم بكتابة رمزها الخاص لاستبدال رمز الملف المصاب، حتى تدمر المحتويات الأصلية للملف. ولذا يتوقف الملف المصاب عن العمل ويتعذر تنظيفه. تعملالفيروسات التطفلية على تعديل الملفات تاركة إياها قيد التشغيل كلياً أو جزئياً. الفيروسات المصاحبة لا تقوم بتعديل الملفات لكنها تقوم بنسخها، وعلى ذلك فإنه عند فتح الملف المصاب يتم تشغيل الملف المنسوخ، أي ملف الفيروس بدلاً من الملف الأصلي. وتشتمل الأنواع الأخرى من الفيروسات على فيروسات الارتباط، وفيروسات OBJ التي التي تصيب وحدات الكائن، وفيروسات LIB التي تصيب مكتبات المترجم، والفيروسات التي تصيب النص الأصلي للبرامج.

فيروس الدودة

بعد اختراق فيروسات الدودة للنظام، يتم تفعيل أحد فيروسات دودة شبكة الاتصال، الذي يشبه الفيروس التقليدي، ويقوم بإجرائه الخبيث. سُميت فيروسات دودة شبكة الاتصال بهذا الاسم نظرًا لقدرتها على الاختراق سرًا من جهاز كمبيوتر إلى جهاز آخر، لنشر نفسها من خلال قنوات معلومات متعددة.

وتصنف فيروسات الدودة حسب طريقة انتشارها الرئيسية المدرجة في الجدول أدناه:

جدول 1. فيروسات الدودة المصنفة حسب طريقة انتشارها

النوع	الاسم	الوصف
فيروس دودة البريد الإلكتروني	فيروسات دودة البريد الإلكتروني	تصيب فيروسات دودة البريد الإلكتروني أجهزة الكمبيوتر عن طريق البريد الإلكتروني. تحتوي الرسالة المصابة على ملف مرفق يحتوى إما على نسخة من فيروس الدودة، أو ارتباط لأحد ملفات فيروسات الدودة المحملة على أحد مواقع الويب. عادةً ما يكون موقع الويب إما موقع تم قرصنته أو يكون هو نفسه موقع قرصنة. يتم تفعيل فيروس الدودة عند فتح الملف المرفق أو عند النقر على الارتباط وتحميل الملف وفتحه يصبح فيروس الدودة فعالاً. يواصل بعد ذلك فيروس الدودة عملية تكاثره من خلال العثور على عناوين بريد إلكتروني أخرى وإرسال رسائل مصابة إلى هذه العناوين.
فيروس دودة المراسلة الفورية	فيروسات دودة المراسلة الفورية	تنتشر فيروسات الدودة هذه من خلال عملاء (المراسلة الفورية) IM مثل ICQ أو MSN Messenger أو AOL Instant Messenger أو Yahoo Pager و Skype. عادة ما تستخدم فيروسات الدودة هذه قوائم اتصال لإرسال رسائل تحتوي على ارتباط لأحد ملفات فيروسات الدودة الموجودة على أحد مواقع الويب. عندما يقوم مستخدم بتحميل ذلك الملف وفتحه، يتم تفعيل فيروس الدودة.

النوع	الاسم	الوصف
فيروسات دودة المحادثة عبر الإنترنت	فيروسات دودة المحادثة عبر الإنترنت	يدخل هذا النوع من فيروسات الدودة إلى الكمبيوتر من خلال قنوات المحادثة عبر الإنترنت، والتي تستخدم في الاتصال مع الآخرين عن طريق الإنترنت في الوقت الفعلي. تقوم فيروسات الدودة هذه بنشر نسخة من ملف فيروس الدودة أو ارتباط لهذا الملف على قناة المحادثة عبر الإنترنت. عندما يقوم المستخدم بتحميل ذلك الملف وفتحه، يتم تفعيل فيروس الدودة.
فيروسات دودة الشبكة	فيروسات دودة شبكة الاتصال (فيروسات دودة تكمن في شبكات اتصال الكمبيوتر)	تنتشر فيروسات الدودة هذه عن طريق شبكات اتصال الكمبيوتر. وتختلف فيروسات دودة شبكة الاتصال عن غيرها من فيروسات الدودة في أنها تنتشر دون تدخل المستخدم. فهي تبحث في شبكة اتصال المنطقة المحلية عن أجهزة كمبيوتر تستضيف برامج تحتوي على نقاط قابلة للاختراق. وتقوم الفيروسات بذلك عن طريق إرسال حزمة شبكة اتصال خاصة (تستغل) احتواءها على رمزها أو جزء منه، إلى كل جهاز كمبيوتر. في حالة وجود كمبيوتر قابل للاختراق في شبكة الاتصال، فسوف يتم اختراقه عن طريق الحزمة. ويتم تفعيل فيروس الدودة بمجرد اختراق الكمبيوتر اختراقاً كاملاً.
فيروس دودة P2P	فيروسات دودة تبادل الملفات	تنتشر فيروسات دودة تبديل الملفات من خلال تبادل الملفات عبر شبكات اتصال النظراء، مثل Kazaa أو Grokster أو EDonkey أو FastTrack أو Gnutella. ولاستخدام شبكة اتصال تبادل الملفات، يقوم فيروس الدودة بنسخ نفسه في مجلد تبادل الملفات الذي يقع عادةً في جهاز كمبيوتر المستخدم. تعرض شبكة اتصال تبادل الملفات معلومات حول الملف ويستطيع المستخدم "العثور" على الملف المصاب في شبكة الاتصال وتحميله وفتحه مثل أي ملف آخر. تقوم فيروسات الدودة الأكثر تعقيداً بمحاكاة بروتوكولات الشبكة الخاصة بشبكة اتصال معينة لتبادل الملفات. وتوفر هذه الفيروسات استجابة إيجابية لطلبات البحث وعرض نسخ من نفسها للتحميل.

النوع	الاسم	الوصف
فيروس الدودة	أنواع أخرى من فيروسات الدودة	فيما يلي أنواع أخرى من فيروسات دودة شبكة الاتصال: • فيروسات الدودة التي يمكنها نشر نُسخ منها عن طريق موارد شبكة الاتصال. وباستخدام مجموعة وظائف نظام التشغيل، تتحرك هذه الفيروسات عبر مجلدات شبكة الاتصال المتاحة وتتصل بأجهزة الكمبيوتر المتصلة بشبكة الاتصال العامة وتحاول فتح أقراصها بغرض الوصول الكامل. وهذه الفيروسات لا تشبه فيروسات دودة شبكات اتصال الكمبيوتر الأخرى، بل يتعين على المستخدم فتح ملف يحتوي على نسخة من فيروس الدودة حتى يتم تفعيله. • فيروسات الدودة التي تستخدم طرق انتشار أخرى ليست مدرجة هنا: على سبيل المثال، فيروسات الدودة التي تنتشر عن طريق الهواتف المحمولة.

برامج حصان طروادة

الفئة الفرعية: برامج حصان طروادة (Trojan_programs)

مستوي الخطورة: مرتفع

برامج حصان طروادة لا تشبه الفيروسات وفيروسات الدودة، فهي لا تنسخ نفسها. وتصيب هذه البرامج الكمبيوتر، على سبيل المثال، عن طريق مرفقات بريد إلكتروني مصابة أو عن طريق استخدام مستعرض ويب عند زيارة المستخدم لموقع ويب "مصاب". ولابد أن يقوم المستخدم ببدء تشغيل برامج حصان طروادة كي تبدأ في تنفيذ إجراءاتها الخبيثة بمجرد تشغيلها.

وتستطيع برامج حصان طروادة القيام بعدد من الإجراءات الخبيثة. وتتمثل الوظائف الرئيسية لبرامج حصان طروادة في منع البيانات وتعديلها ومسحها وفي تعطيل تشغيل أجهزة الكمبيوتر أو شبكات اتصال الكمبيوتر. هذا بالإضافة إلى أن برامج حصان طروادة يمكنها استلام الملفات وإرسالها وتشغيلها إلى جانب عرض الرسائل والوصول إلى صفحات الويب وتحميل البرامج وتثبيتها وإعادة تشغيل الكمبيوتر المصاب.

وغالباً ما يستخدم الدخلاء "مجموعات" تتألف من برامج حصان طروادة متكاملة.

يرد وصف الأنواع المختلفة لبرامج حصان طروادة وسلوكها في الجدول أدناه.

جدول 2. أنواع برامج حصان طروادة المصنفة تبعًا لسلوكها في الكمبيوتر المصاب

النوع	الاسم	الوصف
برامج حصان طروادة لقنابل الأرشيف	برامج حصان طروادة - قنابل الأرشيف	الأرشيف الذي عند فك حزمته يزداد ليصبح بحجم يؤدي إلى تعطيل تشغيل الكمبيوتر. عند محاولة فك حزمة هذا الأرشيف، قد يبدأ الكمبيوتر في العمل ببطء أو "يتجمد"، وقد يتم ملء القرص ببيانات "فارغة". وتمثل "قنابل الأرشيف" خطورة خصوصًا بالنسبة لخوادم البريد الإلكتروني والملفات. في حالة استخدام نظام معالجة للمعلومات الواردة تلقائيًا على الخادم، تستطيع "قنابل الأرشيف" هذه إيقاف تشغيل الخادم.
الباب الخلفي	برامج حصان طروادة للإدارة عن بعد	تعتبر هذه البرامج أخطر أنواع برامج حصان طروادة، والتي تشبه وفقًا لتركيبها الوظيفي البرامج القياسية للإدارة عن بعد. تقوم هذه البرامج بتثبيت نفسها دون علم المستخدم وتتيح للدخيل إمكانية إدارة الكمبيوتر عن بعد.
برامج حصان طروادة	برامج حصان طروادة	من بين برامج حصان طروادة البرامج الخبيثة التالية: • برامج حصان طروادة التقليدية، تقوم فقط بالوظائف الرئيسية لبرامج حصان طروادة: منع البيانات أو تعديلها أو مسحها أو تعطيل تشغيل أجهزة الكمبيوتر أو شبكات اتصال الكمبيوتر. ولا تمتلك خصائص الوظائف الإضافية التي تتمتع بها أنواع برامج حصان طروادة الأخرى الوارد وصفها في هذا الجدول؛ • برامج حصان طروادة "متعددة الأغراض"، يتوافر بها خصائص وظائف إضافية كتلك الخصائص المتاحة في العديد من أنواع برامج حصان طروادة.
برامج حصان طروادة للفدية	برامج حصان طروادة التي تتطلب فدية	هذه البرامج "تأخذ رهينة" معلوماتية على جهاز كمبيوتر المستخدم وتقوم بتعديلها أو منعها أو تعطيل تشغيل الكمبيوتر حتى يتعذر على المستخدم استخدام البيانات. ثم يطلب الدخيل من المستخدم فدية كعوض للتعهد بإرسال البرنامج الذي يعيد قابلية تشغيل الكمبيوتر.

النوع	الاسم	الوصف
برنامج حصان طروادة للتحكم عن بعد	برنامج حصان طروادة للتحكم عن بعد	تقوم هذه البرامج بالوصول إلى صفحات الويب من كمبيوتر المستخدم: فهي ترسل أمرًا إلى مستعرض الويب، أو تستبدل عناوين الويب المخزنة في ملفات النظام. وينظم الدخلاء هجماتهم على شبكة الاتصال باستخدام هذه البرامج ويزيدون من الحركة إلى مواقع معينة لزيادة عوائد عرض الشعارات الإعلانية.
برامج حصان طروادة-أدوات التحميل	برامج حصان طروادة للتحميل	تتمكن هذه البرامج من الوصول إلى صفحة ويب الدخيل، وتحميل برامج خبيثة أخرى منها وتثبيتها على كمبيوتر المستخدم. وتستطيع هذه البرامج إما تخزين الاسم الخاص باسم ملف البرنامج الخبيث القابل للتحميل في رمزها الخاص أو استلام هذا الاسم من صفحة الويب التي تقوم بالوصول إليها.
برامج حصان طروادة للإسقاط	برامج حصان طروادة للإسقاط	تقوم هذه البرامج بحفظ البرامج المحتوية على برامج حصان طروادة الأخرى على قرص جهاز الكمبيوتر ثم تقوم بتثبيتها. يستطيع الدخلاء استخدام برامج حصان طروادة للإسقاط بعدة طرق: • لتثبيت برامج خبيثة دون علم المستخدم: لا تظهر برامج حصان طروادة للإسقاط أية رسائل كما لا تظهر أية رسائل خاطئة مثل الإخطار عن خطأٍ في الأرشيف أو عن استخدام الإصدار الخطأ لنظام التشغيل. • لحماية برنامج خبيث آخر معروف من الاكتشاف: ليس بإمكان جميع برامج مكافحة الفيروسات اكتشاف أي برنامج خبيث متواجد داخل برامج حصان طروادة للإسقاط.

النوع	الاسم	الوصف
برامج حصان طروادة للإخطار	برامج حصان طروادة للإخطار	تقوم هذه البرامج بإخطار الدخيل باتصال جهاز الكمبيوتر المصاب، ومن ثم تنقل إلى الدخيل معلومات عن هذا الكمبيوتر، من بينها: عنوان IP أو رقم المنفذ المفتوح أو عنوان البريد الإلكتروني. وتتصل هذه البرامج بالدخيل مستخدمة عدد من الطرق منها البريد الإلكتروني وعن طريق FTP وبواسطة الوصول إلى صفحة ويب الدخيل. غالباً ما تستخدم برامج حصان طروادة للإخطار في مجموعاتٍ من برامج حصان طروادة التكميلية. وهي تخطر الدخيل بنجاح تثبيت برامج أخرى من حصان طروادة على جهاز كمبيوتر المستخدم.
برامج حصان طروادة لخوادم الوكيل	برامج حصان طروادة لخوادم الوكيل	تتيح للدخيل الوصول إلى صفحات الويب خفية باستخدام هوية مستخدم الكمبيوتر ويتم استخدامها غالباً في إرسال رسائل بريد إلكتروني غير مرغوب فيها.
برامج حصان طروادة لسرقة كلمة المرور	برامج حصان طروادة لسرقة كلمة المرور	برامج حصان طروادة لسرقة كلمة المرور (برمجيات سرقة كلمة المرور)؛ تقوم هذه البرامج بسرقة حسابات المستخدم، مثل معلومات تسجيل البرامج. وهي تعثر على معلومات سرية في ملفات النظام وفي السجل، ثم ترسلها إلى مطورها باستخدام طرق منها البريد الإلكتروني وعن طريق FTP وبالوصول إلى موقع ويب الدخيل. يأتي بعض من برامج حصان طروادة هذه ضمن أنواع معينة واردة في هذا الجدول، وتتضمن حصان طروادة -لسرقة حسابات البنوك وحصان طروادة -لسرقة البيانات الشخصية وحصان طروادة -لسرقة بيانات مستخدمي الألعاب..
برامج Trojan-Spy	برامج حصان طروادة للتجسس	تستخدم هذه البرامج للتجسس على المستخدم: وتقوم بجمع معلومات حول أنشطة المستخدم على الكمبيوتر: فهي على سبيل المثال تعترض البيانات المدخلة من قبل المستخدم عن طريق لوحة المفاتيح وتأخذ لقطة من الشاشة وتجمع قوائم بالتطبيقات النشطة. وبعد استلامها لهذه المعلومات، تقوم بإرسالها إلى الدخيل عن طريق أساليب منها البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى موقع ويب الدخيل.

النوع	الاسم	الوصف
Trojans-DoS	برامج حصان طروادة لهجمات شبكة الاتصال	وبالنسبة لهجوم حجب الخدمة (DoS)، ترسل برامج حصان طروادة العديد من الطلبات من جهاز كمبيوتر المستخدم إلى خادم بعيد. بعد ذلك يستنزف الخادم موارده في معالجة الطلبات ويتوقف عن العمل. تستخدم هذه البرامج غالباً في إصابة أكثر من جهاز كمبيوتر للقيام بهجوم مشترك على الخادم.
برامج حصان طروادة للمراسلات الفورية	برامج حصان طروادة التي تسرق البيانات الشخصية لمستخدمي عميل المراسلة الفورية.	تسرق هذه البرامج أرقام وكلمات مرور مستخدمي عميل المراسلة الفورية (برامج المراسلة الفورية) مثل ICQ أوMSN Messenger أو AOL Instant Messenger أو Yahoo Pager أو Skype. ثم تقوم بنقل المعلومات إلى الدخيل باستخدام طرق منها البريد الإلكتروني وعن طريق FTP وبواسطة الوصول إلى موقع ويب الدخيل.
فيروسات الجذر	فيروسات الجذر	تخفي هذه البرامج برامج خبيثة أخرى كما تخفي نشاطها أيضاً، وبذلك فهي تزيد من وجود هذه البرامج في النظام. وتقوم بإخفاء ملفات وعمليات في ذاكرة جهاز كمبيوتر مصاب أو مفاتيح تسجيل يتم تشغيلها بواسطة برمجيات خبيثة أو تخفي عمليات تبادل البيانات بين التطبيقات المثبتة على جهاز كمبيوتر المستخدم وأجهزة الكمبيوتر الأخرى المتصلة بشبكة الاتصال.
برنامج Trojan-SMS	برامج حصان طروادة لرسائل SMS	تصيب هذه البرامج الهواتف المحمولة وترسل رسائل قصيرة إلى أرقام يدفع مستخدم الهاتف المصاب تكاليف إرسالها.
برامج Trojans-GameThieves	برامج حصان طروادة التي تسرق البيانات الشخصية لمستخدمي ألعاب شبكة الاتصال.	تسرق هذه البرامج معلومات حساب المستخدم الخاصة بمستخدمي ألعاب شبكة الاتصال، و ترسل هذه المعلومات إلى الدخيل باستخدام طرق منها البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى موقع ويب الدخيل.
برامج حصان طروادة لسرقة الحسابات البنكية	برامج حصان طروادة التي تقوم بسرقة معلومات الحسابات البنكية	تسرق هذه البرامج معلومات الحسابات البنكية أو معلومات الحسابات المالية الإلكترونية/الرقمية، وتقوم بإرسال البيانات إلى الدخيل باستخدام طرق منها البريد الإلكتروني وعن طريق FTP وبواسطة الوصول إلى موقع ويب الدخيل.

النوع	الاسم	الوصف
برامج حصان طروادة للبحث عن البريد	برامج حصان طروادة التي تقوم بجمع عناوين البريد الإلكتروني	تقوم هذه البرامج بجمع عناوين البريد الإلكتروني على جهاز الكمبيوتر وإرسالها إلى الدخيل بواسطة طرق منها البريد الإلكتروني أو عن طريق FTP أو بواسطة الوصول إلى موقع ويب الدخيل. يمكن للدخيل استخدام العناوين التي تم جمعها في إرسال بريد إلكتروني غير مرغوب فيه.

أدوات مساعدة خبيثة

الفئة الفرعية: أدوات مساعدة خبيثة (Malicious_tools)

مستوي الخطورة: متوسط

تم تصميم هذه الأدوات المساعدة خصيصاً لإلحاق الضرر. ومع ذلك فإنها أدوات تستخدم في الأساس لمهاجمة أجهزة الكمبيوتر الأخرى على العكس من البرمجيات الخبيثة الأخرى،ويمكن تخزينها وتشغيلها بأمان على كمبيوتر المستخدم. وتوفر هذه البرامج القدرة الوظيفية على المساعدة في إنشاء فيروسات وفيروسات دودة وبرامج حصان طروادة أو في تنظيم هجمات شبكة الاتصال على الخوادم البعيدة أو القرصنة على أجهزة الكمبيوتر أو القيام بأنشطة خبيثة أخرى.

هناك أنواع عديدة من الأدوات المساعدة الخبيثة ذات الوظائف المختلفة والتي تم وصفها في الجدول أدناه.

جدول 3. الأدوات المساعدة الخبيثة المصنفة تبعا للوظائف

النوع	الاسم	الوصف
منشئ فيروسات	منشئو فيروسات	يستخدم منشئو الفيروسات في إنشاء فيروسات جديدة وفيروسات الدودة وبرامج حصان طروادة. ويتوفر لدى بعض منشئي الفيروسات واجهة نوافذ قياسية، مما يتيح للقراصنة اختيار نوع البرنامج الخبيث المطلوب إنشاؤه والطريقة التي سيستخدمها هذا البرنامج في مقاومة التصحيح وغير ذلك من الخصائص المماثلة.
DoS	هجمات شبكة الاتصال	ترسل برامج رفض الخدمة (DoS) العديد من الطلبات من جهاز كمبيوتر المستخدم إلى الخادم البعيد. بعد ذلك سوف يستنزف الخادم موارده في معالجة الطلبات ويتوقف عن

النوع	الاسم	الوصف
		العمل.
فيروس استغلال	فيروسات استغلال	يتكون فيروس الاستغلال من مجموعة بيانات أو جزء من رمز برنامج يستخدم نقاط اختراق تطبيق للقيام بنشاط خبيث على جهاز الكمبيوتر. فعلى سبيل المثال، يمكن لفيروسات الاستغلال كتابة أو قراءة الملفات أو الوصول إلى صفحات ويب "مصابة". تستخدم فيروسات الاستغلال المختلفة نقاط اختراق التطبيقات المختلفة أو خدمات شبكة الاتصال. يتم نقل فيروس الاستغلال عن طريق شبكة الاتصال إلى أجهزة كمبيوتر متعددة على هيئة حزمة شبكة اتصال تبحث عن أجهزة كمبيوتر بها خدمات شبكة اتصال قابلة للاختراق.على سبيل المثال، يبحث فيروس الاستغلال الموجود بأحد ملفات DOC عن مواطن اختراق محرري النصوص، وعندما يقوم المستخدم بفتح أحد الملفات المصابة يستطيع الفيروس تنفيذ الوظائف التي قام الدخيل ببرمجتها. أما فيروس الاستغلال الموجود في رسالة بريد إلكتروني فيقوم بالبحث عن نقاط اختراق برامج عميل بريد إلكتروني، ويمكنه بدء القيام بنشاطه الخبيث بمجرد فتح المستخدم لرسالة مصابة في هذا البرنامج. تستخدم فيروسات الاستغلال أيضاً في توزيع فيروسات دودة الشبكة (الشبكة-فيروسات الدودة). Exploits-Nukers عبارة عن حزم شبكات اتصال تعطل تشغيل أجهزة الكمبيوتر.
مشفرات الملفات	مشفرات الملفات	تقوم مشفرات الملفات بتشفير البرامج الخبيثة الأخرى بغرض إخفائها من تطبيقات مكافحة الفيروسات.
فيروسات إرسال كميات ضخمة من البريد الإلكتروني	برامج تستخدم لإرسال كميات ضخمة من البريد الإلكتروني عبر شبكات الاتصال	تقوم هذه البرامج بإرسال عدد هائل من الرسائل عن طريق قنوات الشبكة، على سبيل المثال قنوات المحادثات عبر الإنترنت. ومع ذلك، لا تحتوي هذه الفئة من البرامج الخبيثة على برامج تقوم بإرسال كميات ضخمة إلى حركة البريد الإلكتروني أو قنوات IM وSMS، والتي تصنف بشكل منفصل في الجدول أدناه (فيروس إرسال كميات ضخمة من البريد الإلكتروني، وفيروس إرسال كميات ضخمة من المراسلات الفورية، وفيروس إرسال كميات ضخمة من الرسائل القصيرة).

النوع	الاسم	الوصف
أدوات القرصنة	أدوات القرصنة	تستخدم أدوات القرصنة في قرصنة أجهزة الكمبيوتر الذي تم تثبيتها عليها، أو في تنظيم هجمات على جهاز كمبيوتر آخر. تحتوي هذه الهجمات على: إنشاء حسابات جديدة لمستخدمي النظام دون الحصول على تصريح، أو مسح سجلات النظام لإخفاء أي تتبعات لوجود مستخدم جديد في النظام. وتتضمن هذه الأدوات بعض برامج مراقبة الشبكة والتي تقوم بوظائف خبيثة، منها على سبيل المثال اعتراض كلمات المرور. وبرامج مراقبة الشبكة عبارة عن برامج تتيح إمكانية فحص حركة شبكة الاتصال.
ليس فيروس: خدعة	برامج خداعية	تفزع هذه البرامج المستخدم بالرسائل التي تشبه الفيروسات: وتقوم هذه البرامج "باكتشاف" فيروس في ملف نظيف، أو عرض رسالة حول عملية لن تحدث لتهيئة قرص مدمج.
برامج محاكية للمستخدم المصرح له	برامج محاكية للمستخدم المصرح له	ترسل هذه البرامج رسائل وطلبات شبكة اتصال بعنوان مرسل مزيف. ويستخدم الدخلاء البرامج المحاكية للمستخدم المصرح له للتظاهر بأنه أحد المرسلين المصرح لهم على سبيل المثال.
أدوات الفيروس	هي أدوات تستخدم لإدخال تعديلات على البرامج الخبيثة	فهي تتيح إمكانية تعديل برامج خبيثة أخرى بغرض إخفائها من تطبيقات مكافحة الفيروسات.
فيروسات إرسال كميات ضخمة من البريد الإلكتروني	برامج إرسال كميات ضخمة من عناوين البريد الإلكتروني	ترسل هذه البرامج عدد هائل من الرسائل إلى عناوين البريد الإلكتروني (غمرها). ونظراً إلى التدفق الضخم من الرسائل، يتعذر على المستخدم عرض الرسائل الواردة غير المرغوب فيها.
فيروسات إرسال كميات ضخمة من المراسلات الفورية	برامج تستخدم لإرسال كميات ضخمة من الرسائل إلى برامج المراسلات الفورية	ترسل هذه البرامج عددًا هائلاً من الرسائل إلى برامج عميل المراسلة الفورية (برامج المراسلة الفورية) مثل ICQ أو MSN Messenger أو AOL Instant Messenger أو Yahoo Pager أو Skype. ونظراً إلى التدفق الضخم من الرسائل، يتعذر على المستخدم عرض الرسائل الواردة غير المرغوب فيها.
فيروسات إرسال كميات ضخمة من الرسائل القصيرة	برامج تستخدم لإرسال كميات ضخمة من الرسائل النصية القصيرة	ترسل هذه البرامج عددًا هائلاً من الرسائل القصيرة إلى الهواتف المحمولة.

برامج يحتمل كونها غير مرغوبة

البرامج التي يحتمل كونها غير مرغوب فيها، لا تشبه البرمجيات الخبيثة، حيث إن الغرض منها لا يقتصر على إلحاق الضرر فقط. وبالرغم من ذلك يمكن استخدام هذه البرامج في اختراق أمان جهاز الكمبيوتر.

من بين البرامج التي يحتمل كونها غير مرغوب فيها البرمجيات الإعلانية والبرمجيات الجنسية وغير ذلك من البرامج التي يحتمل كونها غير مرغوبة.

تعرض البرمجيات الإعلانية (انظر صفحة ٢٦) معلومات إعلانية للمستخدم.

تعرض البرمجيات الجنسية (انظر صفحة ٢٧) معلومات جنسية للمستخدم.

البرمجيات الخطرة الأخرى (انظر صفحة ٢٧) عادة ما تكون هذه البرامج مفيدة ويستخدمها الكثير من مستخدمي الكمبيوتر. غير أنه في حالة وصول دخيل إلى هذه البرامج، أو قيامه بتثبيتها على جهاز كمبيوتر المستخدم، فإن هذا الدخيل يتمكن من استخدامها لخرق أمان جهاز الكمبيوتر.

يتم تثبيت البرامج التي يحتمل كونها غير مرغوبة باستخدام إحدى الطرق التالية:

- يتم تثبيتها بواسطة المستخدم، سواء بمفردها أو مع برنامج آخر. على سبيل المثال، يقوم مطورو البرامج بتضمين برامج إعلانية في البرمجيات المجانية أو البرمجيات المشتركة.
- كما أنه يتم تثبيتها بواسطة الدخلاء أيضاً، فعلى سبيل المثال، يقوم الدخلاء بتضمين هذه البرامج في حزم مع برمجيات خبيثة أخرى مستخدمين "نقاط اختراق" مستعرض الويب أو برامج حصان طروادة للتحميل وبرامج حصان طروادة للإسقاط وذلك عند زيارة المستخدم لموقع ويب "مصاب".

برمجيات إعلانية

الفئة الفرعية: برمجيات إعلانية

مستوي الخطورة: متوسط

تعرض البرمجيات الإعلانية معلومات إعلانية للمستخدم. حيث تعرض هذه البرمجيات شعارات إعلانية في واجهة برنامج آخر، وتعيد توجيه استعلامات البحث إلى مواقع ويب إعلانية. وتقوم بعض البرمجيات الإعلانية بجمع معلومات تسويقية عن المستخدم وإرسالها إلى مطوريها: على سبيل المثال، بالمواقع التي يزورها المستخدم أو بطلبات البحث التي يجريها، ولا تشبه هذه البرمجيات برامج حصان طروادة للتجسس، حيث إنها ترسل تلك المعلومات بتصريح من المستخدم.

برمجيات جنسية

الفئة الفرعية: برمجيات جنسية

مستوي الخطورة: متوسط

يقوم المستخدم بتثبيت هذه البرامج بنفسه عادةً بغرض البحث عن معلومات إباحية أو تحميلها.

ويستطيع الدخلاء أيضًا تثبيت هذه البرامج على جهاز كمبيوتر المستخدم لعرض إعلانات لخدمات ومواقع إباحية تجارية للمستخدم دون الحصول على إذن منه. وحتى يتم تثبيتها، يستخدم الدخلاء نقاط اختراق نظام التشغيل أو مستعرض الويب، ويقومون بنشرها عادةً من خلال برامج حصان طروادة للتحميل وبرامج حصان طروادة للإسقاط.

يوجد ثلاثة أنواع من البرمجيات الجنسية وفقًا للتصنيف الوارد في الجدول التالي.

جدول 4. أنواع البرمجيات الجنسية وفقاً لتصنيف وظائفها

النوع	الاسم	الوصف
برامج الاتصال الجنسية	برامج الاتصال التلقائي	تحتوي هذه البرامج على أرقام الهاتف الخاصة بالخدمات الإباحية عبر الهاتف وتقوم بالاتصال تلقائيًا بتلك الخدمات؛ وهي لا تشبه برامج حصان طروادة التي للاتصال، لأنها تخبر المستخدم بإجراءاتها.
أدوات التحميل الجنسية	برامج تحميل ملفات من الإنترنت	تقوم هذه البرامج بتحميل معلومات إباحية إلى جهاز كمبيوتر المستخدم؛ وهي لا تشبه برامج حصان طروادة التي للاتصال، لأنها تخبر المستخدم بإجراءاتها.
الأدوات الجنسية	الأدوات	تستخدم هذه الأدوات في البحث عن مواد إباحية وعرضها؛ ويتضمن هذا النوع أشرطة أدوات مستعرض خاص ومشغلات فيديو خاصة.

برمجيات خطرة أخرى

الفئة الفرعية: برمجيات خطرة أخرى

مستوي الخطورة: متوسط

تتميز معظم هذه البرامج بأنها برامج مفيدة وذلك في الاستخدام الشائع المصرح به. وهي تتضمن عملاء المحادثة عبر الإنترنت وبرامج الاتصال وبرامج إدارة تحميل الملفات وبرامج مراقبة أنشطة نظام الكمبيوتر والأدوات المساعدة لإدارة كلمات المرور وFTP أو HTTP أو خوادم Telnet.

غير أنه في حالة وصول دخيل إلى هذه البرامج، أو قيامه بتثبيتها على جهاز كمبيوتر المستخدم، فإنه من الممكن استخدام وظيفة هذه البرامج لخرق أمان جهاز الكمبيوتر.

يعرض الجدول البرمجيات الخطرة والمصنفة وفقًا لوظائفها.

جدول 5. أنواع أخرى من البرمجيات الخطرة مصنفة طبقًا لوظائفها

النوع	الاسم	الوصف
عميل IRC	برامج عميل المحادثة عبر الإنترنت	يقوم المستخدم بتثبيت هذه البرامج للاتصال من خلال قنوات المحادثة عبر الإنترنت. ويستخدم الدخلاء هذه البرامج لنشر البرمجيات الخبيثة.
برامج الاتصال	برامج الاتصال التلقائي	ويمكن لهذه البرامج إنشاء اتصالات هاتفية "خفية" عن طريق المودم.
أدوات التحميل	أدوات التحميل	يمكن لهذه البرامج تحميل ملفات من مواقع الويب سرًا.
برامج المراقبة	برامج المراقبة	تراقب هذه البرامج أنشطة أجهزة الكمبيوتر المثبتة عليها، بما في ذلك مراقبة أداء التطبيقات، وعمليات تبادل البيانات باستخدام تطبيقات مثبتة على أجهزة كمبيوتر أخرى.
أدوات سرقة كلمة المرور	أدوات استعادة كلمة المرور	تستخدم هذه البرامج لعرض واستعادة كلمات المرور المنسية. يستخدم الدخلاء هذه البرامج بنفس الطريقة التي يستخدمونها عند قيامهم بتثبيتها على أجهزة الكمبيوتر الخاصة بالمستخدم.
الإدارة عن بعد	برامج الإدارة عن بعد	تستخدم هذه البرامج من قبل مسئولي النظام غالبًا؛ فهي تتيح الوصول إلى كمبيوتر بعيد، بغرض مراقبته وإدارته. يستخدم الدخلاء هذه البرامج بنفس الطريقة التي يستخدمونها عند قيامهم بتثبيتها على أجهزة الكمبيوتر الخاصة بالمستخدم. تختلف البرامج الخطرة للإدارة عن بعد عن برامج حصان طروادة (أو الباب الخلفي) للإدارة عن بعد. تستطيع برامج حصان طروادة التسلل بمفردها إلى النظام وتثبيت نفسها؛ بينما لا تتوافر مثل هذه الوظائف في البرمجيات الشرعية.
خادم FTP	خوادم FTP	تقوم هذه البرامج بوظائف خوادم FTP. ويقوم الدخلاء بتثبيتها على أجهزة كمبيوتر المستخدمين للحصول على إمكانية الوصول عن بعد عن طريق بروتوكول FTP.

النوع	الاسم	الوصف
خادم-وكيل	خوادم الوكيل	تؤدي هذه البرامج وظائف خوادم الوكيل. ويقوم الدخلاء بتثبيتها على أجهزة كمبيوتر المستخدمين لإرسال بريد إلكتروني غير مرغوب فيه من خلال تلك الأجهزة
خادم-Telnet	خوادم Telnet	تؤدي هذه البرامج وظائف خوادم Telnet. ويقوم الدخلاء بتثبيتها على أجهزة كمبيوتر المستخدمين للحصول على إمكانية الوصول عن بعد عن طريق بروتوكول Telnet.
خادم ويب	خوادم الويب	تؤدي هذه البرامج وظائف خوادم الويب. ويقوم الدخلاء بتثبيتها على أجهزة كمبيوتر المستخدمين للحصول على إمكانية الوصول عن بعد عن طريق بروتوكول HTTP.
RiskTool	أدوات الكمبيوتر المحلية	توفر هذه الأدوات للمستخدم وظائف إضافية ولا تستخدم إلا على جهاز كمبيوتر المستخدم. فهي تسمح للقراصنة بإخفاء ملفات، أو إخفاء نوافذ تطبيقات فعالة، أو إغلاق عمليات فعالة.
NetTool	أداوت شبكة الاتصال	تتيح هذه الأدوات لمستخدم الكمبيوتر إدارة أجهزة الكمبيوتر الأخرى المتصلة بالشبكة عن بعد: تقوم هذه الأدوات، على سبيل المثال، بإعادة تشغيل أجهزة الكمبيوتر أو العثور على منافذ مفتوحة أو تشغيل برامج مثبتة عليها.
عميل P2P	برامج عميل النظراء	تستخدم هذه البرامج لإدارة شبكات اتصال النظراء. ويستطيع الدخلاء استخدام هذه البرامج لنشر برمجيات خبيثة.
عميل SMTP	عملاء SMTP	ترسل هذه البرامج رسائل بريد إلكتروني وتخفي هذا النشاط. ويقوم الدخلاء بتثبيتها على أجهزة كمبيوتر المستخدمين لإرسال بريد إلكتروني غير مرغوب فيه مستخدمين في ذلك هويات المستخدمين.
WebToolbar	أشرطة أدوات الويب	تضيف هذه البرامج أشرطة أدوات البحث الخاصة بها إلى أشرطة أدوات مستعرضات أخرى.

النوع	الاسم	الوصف
FraudTool	برامج خداعية	تظهر هذه البرامج بصورة برامج حقيقية. فعلى سبيل المثال، تعرض البرامج الاحتيالية لمكافحة الفيروسات رسائل حول اكتشاف برمجيات خبيثة، مع أنها لم تعثر على أي شيء أو لم تقم بتنظيف أي شئ.

طرق اكتشاف التطبيق للكائنات المصابة والمشكوك فيها والتي يحتمل كونها خطرة

يستخدم برنامج مكافحة الفيروسات من Kaspersky طريقتين لاكتشاف البرمجيات الخبيثة المتواجدة بالكائنات: تفاعلية (باستخدام قواعد البيانات) و وقائية (باستخدام التحليل المساعد على الاكتشاف).

تحتوي قواعد بيانات التطبيق على سجلات تُستخدم للتعرف على أي من مئات الآلاف من التهديدات المعروفة في الكائنات التي تم فحصها. وتحتوي هذه السجلات على معلومات حول كل من أقسام التحكم في رمز البرمجيات الخبيثة والخوارزميات المستخدمة في تنظيف الكائنات التي تحتوي على هذه البرمجيات. يقوم محللوا مكافحة الفيروسات في Kaspersky Lab بتحليل مئات البرمجيات الخبيثة الجديدة بشكل يومي وإنشاء سجلات لتعريفها وتضمينها في تحديثات ملفات قاعدة البيانات.

إذا اكتشف برنامج مكافحة الفيروسات من Kaspersky أقسام من رمز في كائن تم فحصه تتوافق كلياً مع أقسام رمز التحكم لبرنامج خبيث وفقاً لأحد سجلات قاعدة البيانات، فإنه يحدد حالة الكائن على أنه مصاب: وإذا كان هناك توافق جزئي، فإنه يحدد حالة الكائن على أنه مشكوك فيه.

وباستخدام الطريقة الوقائية، يستطيع التطبيق اكتشاف البرمجيات الخبيثة الجديدة التي لم تُدرج بعد في قاعدة البيانات.

يكتشف التطبيق كائنات تحتوي على برمجيات خبيثة جديدة وفقاً لسلوك هذه الكائنات. قد لا يتوافق رمز البرنامج الخبيث الجديد بشكل كلي أو حتى جزئي مع رمز برنامج خبيث معروف، ولكنه قد يحتوي على تسلسلات أوامر مميزة مثل فتح ملف أو الكتابة فيه أو اعتراض متجهات المقاطعة. وعلي سبيل المثال، يستطيع التطبيق تحديد ما إذا كان الملف مصاباً بفيروس تمهيد غير معروف أم لا.

يتم إعطاء الكائنات التي يتم اكتشافها باستخدام الطريقة الوقائية حالة يحتمل كونها خطرة.

تثبيت التطبيق

يتم تثبيت التطبيق على جهاز الكمبيوتر في الوضع التفاعلي باستخدام معالج إعداد التطبيق.

تحذير!

نوصي بإغلاق كافة التطبيقات قيد التشغيل قبل متابعة التثبيت.

لتثبيت التطبيق على جهاز الكمبيوتر، قم بتشغيل ملف التوزيع، والذي يحتوي على ملف بامتداد exe.

ملاحظة

تثبيت التطبيق من ملف التثبيت الذي تم تحميله عن طريق الإنترنت مماثل تماماً لتثبيت التطبيق من القرص المدمج.

يتم تنفيذ برنامج الإعداد في صورة معالج قياسي بنظام Windows. وتحتوي كل نافذة على مجموعة من الأزرار للتحكم في عملية التثبيت. فيما يلي وصف موجز لأغراض هذه الأزرار.

- **التالي** - قبول الإجراء والانتقال إلى الخطوة التالية في عملية التثبيت.
- **السابق** – العودة إلى الخطوة السابقة في عملية التثبيت.
- **إلغاء** – إلغاء التثبيت.
- **إنهاء** – إنهاء إجراء تثبيت التطبيق.

فيما يلي وصف مفصل لكل خطوة من خطوات تثبيت الحزمة.

في هذا القسم:

الخطوة 1. البحث عن إصدار أحدث من التطبيق

قبل تثبيت التطبيق على جهاز الكمبيوتر، يقوم المعالج بالدخول على خوادم تحديث Kaspersky Lab للتحقق من وجود إصدار أحدث.

إذا لم يتم اكتشاف إصدار أحدث من التطبيق على خوادم تحديث Kaspersky Lab، سيبدأ تشغيل معالج الإعداد وسوف يتم تثبيت الإصدار الحالي.

إذا تمَّ اكتشاف إصدار أحدث من التطبيق على خوادم تحديث Kaspersky Lab، سوف يطلب منك ما إذا كنت ترغب في تحميلها وتثبيتها. وإذا قمت بإلغاء التحميل، سيبدأ تشغيل معالج الإعداد لتثبيت الإصدار الحالي. أما إذا قررت تثبيت الإصدار الأحدث من التطبيق، فسوف يتم تحميل ملفات التثبيت إلى جهاز الكمبيوتر وسيبدأ تشغيل معالج الإعداد تلقائياً لتثبيت الإصدار الأحدث. لمزيد من التفاصيل بشأن تثبيت إصدار أحدث من التطبيق، الرجاء الرجوع إلى وثائق ذلك الإصدار.

الخطوة 2. التحقق من استيفاء النظام لمتطلبات التثبيت.

قبل تثبيت التطبيق على جهاز الكمبيوتر، يقوم المعالج بالتحقق من أن الكمبيوتر يلبي الحد الأدنى من متطلبات التثبيت (انظر القسم "متطلبات النظام من الأجهزة والبرامج" في صفحة ١٢). كما سيتأكد من أنه لديك الحقوق اللازمة لتثبيت البرنامج على الجهاز.

في حالة عدم استيفاء أي من المتطلبات، سيظهر على الشاشة إخطار يفيد بذلك. نوصي المستخدم بتثبيت التحديثات المطلوبة باستخدام خدمة **Windows Update** وكذلك البرامج المطلوبة قبل محاولة تثبيت برنامج مكافحة الفيروسات من Kaspersky مرة أخرى.

الخطوة 3. نافذة تحية المعالج

إذا كان النظام يلبي متطلبات النظام (انظر القسم "متطلبات النظام من الأجهزة والبرامج" في صفحة ١٢)، ولم يتم العثور على إصدار أحدث من التطبيق على خوادم تحديث Kaspersky Lab أو إذا قام المستخدم بإلغاء تثبيت ذلك الإصدار، فسوف يبدأ تشغيل معالج الإعداد لتثبيت الإصدار الحالي من التطبيق.

سيظهر على الشاشة أول مربع حوار لمعالج الإعداد مشيراً إلى قرب بدء التثبيت.

لمتابعة التثبيت، اضغط زر التالي. لإلغاء التثبيت، اضغط زر **إلغاء**.

الخطوة 4. استعراض اتفاقية الترخيص

يحتوي مربع حوار المعالج التالي على اتفاقية الترخيص التي يتم إبرامها بين المستخدم وشركة Kaspersky Lab. اقرأ اتفاقية الترخيص بعناية وفي حالة موافقتك على جميع البنود والشروط الواردة بها، قم بتحديد خيار **أقبل بشروط اتفاقية الترخيص** ثم اضغط زر التالي. سيتم متابعة التثبيت.

لإلغاء التثبيت، اضغط زر **إلغاء**.

الخطوة 5. تحديد نوع التثبيت

أثناء هذه الخطوة، سيطلب من المستخدم تحديد نوع التثبيت الأنسب له:

- **تثبيت سريع**. إذا قام المستخدم بتحديد هذا الخيار، فسوف يتم تثبيت التطبيق الكامل على جهاز الكمبيوتر مع إعدادات الحماية الافتراضية الموصى بها من قبل Kaspersky Lab. وبمجرد اكتمال التثبيت، يبدأ تشغيل معالج تكوين التطبيق.
- **تثبيت مخصص**. إذا قمت بتحديد هذا الخيار، سوف يطلب منك: لتحديد مكونات التطبيق التي ترغب في تثبيتها؛ ولتحديد المجلد الذي سيتم تثبيت التطبيق به (انظر القسم " تحديـد مجلـد .6 الخطـوة تـالتثـــبي" في صفحة ٣٥)، ولتفعيل التطبيق وتكوينه باستخدام معالج تكوين التطبيق.

في حالة تحديد الخيار الأول، فسوف ينتقل معالج تثبيت التطبيق مباشرة إلى الخطوة 8 (انظر القسم " .8 الخطـوة تـالبحـث عـن بـرامج أخـرى لمكافحـة الفيروسـا" في صفحة ٣٦). وإلا فسوف يطلب من المستخدم إدخال خيار أو القيام بالتأكيد في كل خطوة من التثبيت.

الخطوة 6. تحديد مجلد التثبيت

> ملاحظة
>
> لن يتم إجراء هذه الخطوة من معالج التثبيت إلا إذا حدد المستخدم خيار التثبيت المخصص (انظر القسم " .5 الخطـوة تحديـــد نـــوع التثبيـــت" بصفحة ٣٤).

أثناء هذه الخطوة، سوف يُطلب من المستخدم تحديد مجلد على جهاز الكمبيوتر ليتم تثبيت التطبيق به. المسار الافتراضي هو:

- **<Drive> \ Program Files \ Kaspersky Lab \ برنامج مكافحة الفيروسات 2009 من Kaspersky** – بالنسبة للأنظمة 32 بت.
- **<Drive> \ Program Files (x86) \ Kaspersky Lab \ برنامج مكافحة الفيروسات 2009 من Kaspersky** – بالنسبة للأنظمة 64 بت.

يتاح للمستخدم إمكانية تحديد مجلد مختلف بالضغط على زر استعراض وتحديد مجلد في مربع حوار تحديد مجلد القياسي أو بإدخال مسار المجلد إليه في حقل الإدخال المتاح.

> تحذير!
>
> الرجاء ملاحظة أنه في حالة القيام بإدخال المسار إلى مجلد التثبيت بالكامل يدوياً، فينبغي ألا يزيد طوله عن 200 حرفاً وألا يحتوي على حروف خاصة.

لمتابعة التثبيت، اضغط زر التالي.

الخطوة 7. تحديد مكونات التطبيق المطلوب تثبيتها

ملاحظة. لن يتم إجراء هذه الخطوة من معالج التثبيت إلا إذا حدد المستخدم خيار التثبيت المخصص (انظر القسم "تحديد نوع التثبيت .5 الخطوة" بصفحة ٣٤).

أثناء أيٍ من حالات التثبيت المخصص، يجب على المستخدم تحديد أي مكونات التطبيق يرغب في تثبيتها على جهاز الكمبيوتر. يتم تحديد كافة مكونات التطبيق بشكلٍ افتراضي: مكونات الحماية والفحص والتحديث.

توجد بعض المعلومات عن كل مكون لمساعدتك في تحديد أيٍ من المكونات التي ترغب في تثبيتها: حدد المكون من القائمة واطلع على المعلومات المتاحة في الحقل أدناه. تتضمن المعلومات وصفاً موجزاً للمكون والمساحة الخالية بالقرص الثابت اللازمة لتثبيته.

لمنع تثبيت أي مكون، افتح قائمة الاختصار بالنقر على الأيقونة المجاورة لاسم المكون وحدد عنصر **"المكون لن يكون متاحاً"**. لاحظ أنه في حالة إلغاء تثبيت أي مكون، فلن يكون جهاز الكمبيوتر محمياً ضد عدد من البرامج الخطرة.

لتحديد أي مكون ليتم تثبيته، افتح قائمة الاختصار بالنقر على الأيقونة المجاورة لاسم المكون وحدد عنصر **"سيتم تثبيت المكون على القرص الثابت المحلي"**.

بعد الانتهاء من تحديد المكونات، اضغط زر التالي . للعودة إلى القائمة الافتراضية للمكونات التي سيتم تثبيتها، اضغط زر فحص .

الخطوة 8. البحث عن برامج أخرى لمكافحة الفيروسات

أثناء هذه الخطوة، يقوم المعالج بالبحث عن برامج أخرى لمكافحة الفيروسات من بينها برامج Kaspersky Lab الأخرى، التي قد تتعارض مع هذا التطبيق.

في حالة اكتشاف أي من تلك البرامج على جهاز الكمبيوتر، فسوف يتم عرض قائمة بها على الشاشة. وسوف يطلب من المستخدم إلغاء تثبيتها قبل متابعة التثبيت.

يمكن للمستخدم الاختيار بين إزالة هذه البرامج تلقائياً أو يدوياً باستخدام أدوات التحكم الموجودة أسفل قائمة برامج المكتشفة لمكافحة الفيروسات.

إذا احتوت قائمة البرامج المكتشفة لمكافحة الفيروسات على الإصدار 7.0 من التطبيق Kaspersky Lab، يتعين على المستخدم حفظ ملف مفتاح ذلك البرنامج عند إلغاء تثبيته. يمكن استخدام هذا المفتاح مع الإصدار الحالي من التطبيق. كما نوصي بحفظ الكائنات المخزنة في العزل وفي مخزن النسخ الاحتياطي؛ وسيتم نقلها إلى العزل في الإصدار الحالي تلقائياً، وستتاح للمستخدم إمكانية إعادة فحصها بعد التثبيت.

في حالة تحديدك الحذف التلقائي للإصدار 7.0، سيتم حفظ المعلومات المتعلقة بتفعيله، وسيعاد استخدامها أثناء تثبيت إصدار 2009.

> تحذير!
>
> يقبل التطبيق ملفات المفتاح الخاصة بالإصدارين 6.0 و 7.0. ملفات المفتاح المستخدمة مع الإصدار 5.0 وما قبله غير مدعمة.

لمتابعة التثبيت، اضغط زر التالي.

الخطوة 9. الإعداد النهائي للتثبيت

تكمل هذه الخطوة الإعداد لتثبيت التطبيق على جهاز الكمبيوتر الخاص بك.

عندما تقوم بتثبيت التطبيق المخصص للمرة الأولى (انظر القسم "تحديد نوع التثبيت .5 الخطوة" في صفحة ٣٤) نوصي بعدم إلغاء تحديد مربع **تمكين الدفاع الذاتي قبل التثبيت**. سوف يتيح لك تمكين هذا الخيار القيام بإجراء العودة إلى التثبيت الصحيح.عند حدوث خطأ أثناء التثبيت. عند إعادة محاولة التثبيت، نوصي بحذف العلامة من أمام ذلك المربع.

> ملاحظة
>
> في حالة تثبيت التطبيق عن بعد باستخدام **سطح المكتب البعيد**، ننصحك بإلغاء تحديد مربع **تمكين الدفاع الذاتي قبل التثبيت**. إذا تم وضع علامة أمام هذا المربع، فقد يتم القيام بإجراء التثبيت بطريقة خاطئة أو لن يتم القيام به إطلاقاً.

لمتابعة التثبيت، اضغط زر التالي. وسوف يبدأ نسخ ملفات التثبيت إلى جهاز الكمبيوتر.

> تحذير!
>
> أثناء عملية التثبيت، سيتم قطع اتصال شبكة الاتصال الحالي إذا اشتملت حزمة التطبيق على مكونات لاعتراض حركة شبكة الاتصال. سيتم استعادة غالبية الاتصالات التي تم إنهاؤها في الوقت المناسب.

الخطوة 10. إنهاء التثبيت

تحتوي نافذة **اكتمال التثبيت** على معلومات حول إتمام تثبيت التطبيق على جهاز الكمبيوتر.

على سبيل المثال، ستبين هذه النافذة ما إذا كان من الضروري إعادة تشغيل الكمبيوتر لإكمال التثبيت بصورة صحيحة. وبعد إعادة تشغيل النظام، سيبدأ تشغيل معالج الإعداد تلقائياً.

إذا لم يكن من الضروري إعادة تشغيل النظام، اضغط زر التالي لبدء معالج تكوين التطبيق.

واجهة التطبيق

يتمتع التطبيق بواجهة بسيطة وسهلة الاستخدام إلى حد ما. يناقش هذا الفصل الميزات الأساسية لواجهة التطبيق بالتفصيل.

وبالإضافة إلى واجهة التطبيق الرئيسية، هناك مكونات إضافية لبرنامج Microsoft Outlook وبرنامج The Bat! وبرنامج Microsoft Windows Explorer. تزيد المكونات الإضافية من مجموعة وظائف هذه البرامج، حيث إنها تتيح إمكانية إدارة وتكوين مكونات برنامج مكافحة الفيروسات من Kaspersky من واجهة برنامج العميل.

في هذا القسم:

رمز منطقة الإخطار

فور تثبيت التطبيق مباشرة، سيظهر رمز التطبيق في منطقة شريط مهام Microsoft Windows.

يشير هذا الرمز إلى العملية الحالية التي يجريها التطبيق. كما يعكس هذا الرمز حالة الحماية ويعرض عددًا من الوظائف الأساسية التي يقوم بها البرنامج.

إذا كان الرمز نشطاً (ملوناً)، فهذا يعني أن كل مكونات الحماية أو بعضها قيد التشغيل. أما إذا كان الرمز غير نشط (أبيض وأسود)، فهذا يعني أن جميع مكونات الحماية معطلة.

يتغير رمز التطبيق وفقاً لإجراء التشغيل الجاري:

– بريد إلكتروني قيد الفحص.

– تحديث قواعد بيانات التطبيق ووحدات البرنامج.

– يحتاج الكمبيوتر إلى إعادة التمهيد لتطبيق التحديثات.

– حدث خطأ في بعض مكونات برنامج مكافحة الفيروسات من Kaspersky.

كما يتيح الرمز إمكانية الوصول إلى أساسيات واجهة البرنامج، بما في ذلك قائمة الاختصار (انظر القسم " قائمة الاختصار" بصفحة ٤٠) و نافذة التطبيق الرئيسية (انظر القسم "نافذة التطبيق الرئيسية" بصفحة ٤١).

لفتح قائمة الاختصار، انقر بزر الماوس الأيمن على رمز التطبيق.

لفتح نافذة التطبيق الرئيسية، انقر نقراً مزدوجاً على رمز التطبيق. دائماً ما تظهر النافذة الرئيسية في قسم الحماية.

في حال توفر أخبار من Kaspersky Lab، فسوف يظهر رمز الأخبار في منطقة إخطار شريط المهام . انقر نقراً مزدوجاً على الرمز لعرض الأخبار في النافذة التي ستظهر.

قائمة الاختصار

يمكن تشغيل مهام الحماية الأساسية من قائمة السياق التي تحتوي على هذه العناصر:

- **تحديث** – بدء تحديثات وحدة التطبيق وقاعدة البيانات وتثبيت التحديثات على جهاز الكمبيوتر الخاص بك.
- **فحص كامل للكمبيوتر** – بدء فحص كلي لجهاز الكمبيوتر للبحث عن كائنات خطرة. سيتم فحص الكائنات الكامنة في كافة الأقراص، بما فيها وسائط التخزين القابلة للإزالة.
- **فحص الفيروسات** – تحديد كائنات وبدء فحص الفيروسات. تحتوي القائمة الافتراضية لهذا الفحص على كائنات عديدة، مثل مجلد **My documents** وأرشيف البريد الإلكتروني. يمكنك إضافة كائنات أخرى إلى هذه القائمة لكي يتم فحصها وذلك عن طريق تحديدها.
- **برنامج مكافحة الفيروسات من Kaspersky** – فتح نافذة التطبيق الرئيسية (انظر القسم " نافذة التطبيق الرئيسية" في صفحة ٤١).
- **الإعدادات** - استعراض وتعديل إعدادات التطبيق.
- **تفعيل** – تفعيل البرنامج. ولكي تصبح عضوًا مسجلا، يتعين عليك تفعيل التطبيق الخاص بك. لا يتاح عنصر القائمة هذا إلا إذا تم إلغاء تفعيل التطبيق.
- **حول** – عرض معلومات حول التطبيق.

- **إيقاف الحماية مؤقتًا / استئناف الحماية** – تعطيل أو تمكين مكونات الحماية في الوقت الفعلي مؤقتًا. لا يؤثر خيار القائمة هذا على تحديثات التطبيق أو تنفيذ مهام فحص الفيروسات.
- **إنـهاء** – إغلاق التطبيق وإلغاء تحميله من ذاكرة الكمبيوتر.

تحديث
فحص كامل للكمبيوتر
فحص الفيروسات...

Kaspersky Anti-Virus
الإعدادات
تفعيل...
حول

إيقاف الحماية مؤقتاً...

إنـهاء

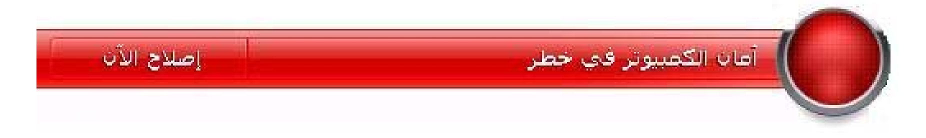
الرسم التوضيحي 1: قائمة الاختصار

إذا تمَّ فتح قائمة الاختصار أثناء إجراء مهمة لفحص الفيروسات، فسوف يظهر في قائمة الاختصار اسم هذه المهمة وحالة تقدم سيرها (النسبة المئوية المكتملة). وعند تحديد المهمة، سوف يتاح لك فتح نافذة التطبيق الرئيسية التي تحتوي على تقرير حول النتائج الحالية لتنفيذ المهمة.

نافذة التطبيق الرئيسية

يمكن تقسيم نافذة التطبيق الرئيسية إلى ثلاثة أجزاء:

- يشير الجزء العلوي من الإطار إلى حالة الحماية الحالية لجهاز الكمبيوتر.



- *الرسم التوضيحي 2. حالة الحماية الحالية لجهاز الكمبيوتر*

هناك ثلاث قيم ممكنة لحالة الحماية: وتتم الإشارة إلى كل حالة بلون معين مشابه لأحد ألوان إشارة المرور. يشير اللون الأخضر إلى أن حماية الكمبيوتر عند المستوي الصحيح، بينما يشير كل من اللونين الأصفر والأحمر إلى وجود تهديدات أمنية في تكوين النظام أو في تشغيل التطبيق. وتشمل

التهديدات، إلى جانب البرامج الخبيثة، قواعد بيانات التطبيقات المهملة ومكونات الحماية المعطلة وتحديد الحد الأدنى من إعدادات الحماية.

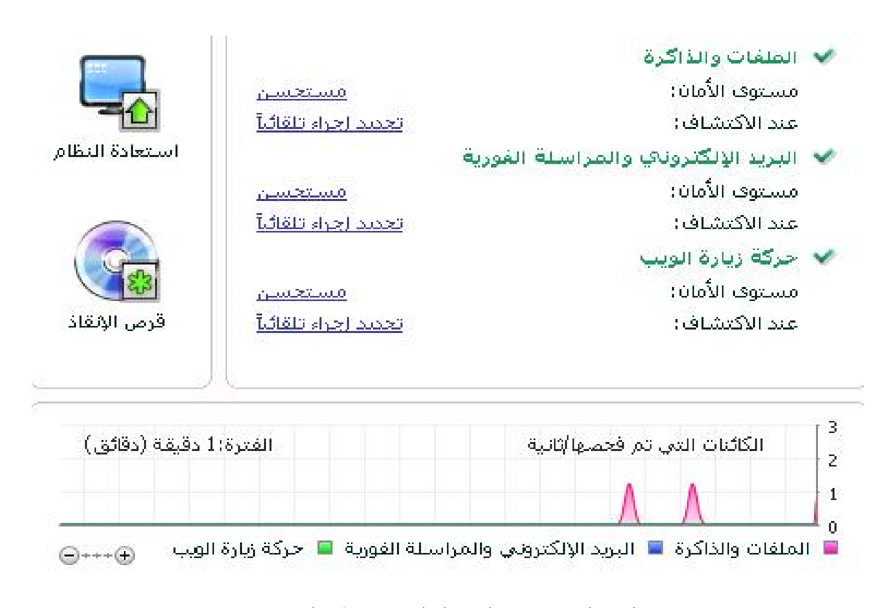
يجب إزالة تهديدات الأمان بمجرد ظهورها. للحصول على معلومات تفصيلية حول تهديدات الأمان وسرعة إزالتها، استخدم ارتباط إصلاح الآن (انظر الرسم التوضيحي السابق).

- يوفر شريط التنقل الموجود بالجزء الأيمن من النافذة وصولاً سريعاً لوظائف التطبيق، بما فيها من مهام فحص لمكافحة الفيروسات ومهام التحديث.



الرسم التوضيحي 3. الجزء الأيمن من النافذة الرئيسية

- يحتوي الجزء الأيسر من النافذة على معلومات حول وظيفة التطبيق المحددة في الجزء الأيمن ويستخدم لتكوين هذه الوظائف وعرض أدوات للقيام بمهام الفحص لمكافحة الفيروسات وتحميل التحديثات وما شابه.



الرسم التوضيحي 4: الجزء المعلوماتي بالإطار الرئيسي

يمكنك أيضاً استخدام هذه الأزرار:

- الإعدادات - لفتح نافذة تكوين التطبيق.
- تعليمات - لفتح نظام تعليمات التطبيق.
- المكتَشَف - لفتح قائمة الكائنات الضارة التي تم اكتشافها بواسطة أي مكون أو مهمة فحص ولعرض إحصائيات مفصَّلة عن تشغيل التطبيق.
- التقارير - لفتح قائمة الأحداث التي تمت أثناء تشغيل التطبيق.
- الدعم - لعرض معلومات حول النظام وارتباطات بمصادر معلومات Kaspersky Lab، بما في ذلك موقع خدمة الدعم الفني والمنتدى.

ملاحظة

يمكنك تغيير مظهر التطبيق من خلال إنشاء واستخدام أنظمة الألوان والرسومات الخاصة بك.

إخطارات

إذا وقعت أحداث أثناء تشغيل التطبيق، سوف تظهر على الشاشة إخطارات خاصة في شكل رسائل منبثقة فوق رمز التطبيق في شريط مهام Microsoft Windows.

ووفقاً لدرجة حرج الحدث بالنسبة لأمان الكمبيوتر، فربما يتلقى المستخدم الأنواع التالية من الإخطارات:

- تنبيه. وقع حدث هام؛ على سبيل المثال تم اكتشاف فيروس أو نشاط خطر في النظام. ينبغي أن يقرر المستخدم على الفور كيفية التعامل مع هذا التهديد. يظهر هذا النوع من الإخطارات باللون الأحمر.
- تحذير! وقع حدث يحتمل أن يكون خطرًا. على سبيل المثال، تم اكتشاف ملفات يحتمل كونها مصابة أو نشاط مشكوك فيه في النظام. يجب على المستخدم توجيه البرنامج وفقاً لمدى تقديره لخطورة ذلك الحدث. يظهر هذا النوع من الإخطارات باللون الأصفر.
- ملاحظة: يعطي هذا الإخطار معلومات حول الأحداث غير الحرجة. ويتضمن هذا النوع، على سبيل المثال؛ الإخطارات المتعلقة بتشغيل مكون تصفية المحتوى. تظهر الإخطارات الإعلامية باللون الأخضر.

نافذة إعدادات التطبيق

يمكن فتح نافذة إعدادات التطبيق من نافذة التطبيق الرئيسية (انظر القسم "نافـــذة التطبيـــق الرئيســـية " في صفحة ٤١) أو قائمة الاختصار (انظر القسم "قائمـــة الاختصـــار" في صفحة ٤٠). لفتح النافذة، انقر رابط الإعدادات أعلى نافذة التطبيق الرئيسية، أو حدد الخيار المناسب من قائمة الاختصار الخاصة بالتطبيق.

تتكون نافذة تكوين الإعدادات من جزأين:

- الجزء الأيمن من النافذة يتيح الوصول إلى مكونات التطبيق، مثل مهام فحص الفيروسات ومهام التحديث،
- الجزء الأيسر من النافذة يحتوي على قائمة من إعدادات المكون أو المهمة المحددة في الجزء الأيمن من النافذة.

البداية

يتمثل أحد الأهداف الأساسية لشركة Kaspersky Lab في تقديم التكوين الأمثل لكافة خيارات التطبيق عند إنشاء برنامج مكافحة الفيروسات من Kaspersky. ويتيح ذلك لمستخدم الكمبيوتر غير المحترف حماية جهاز الكمبيوتر الخاص به فور التثبيت دون قضاء ساعات في تغيير الإعدادات.

وحرصاً منا على راحة المستخدم، قمنا بدمج مراحل التكوين الأولي معاً في الإعداد الأولي الموحد والذي يبدأ بمجرد تثبيت التطبيق. ويمكنك بإتباع تعليمات المعالج تفعيل التطبيق وتكوين الإعدادات من أجل التحديثات وتقييد الوصول إلى البرنامج باستخدام كلمة مرور إلى جانب القيام بإعدادات أخرى.

يمكن إصابة جهاز الكمبيوتر ببرمجيات خبيثة قبل تثبيت التطبيق. لاكتشاف البرمجيات الخبيثة الموجودة، قم بإجراء فحص الكمبيوتر(انظر القسم "فحص الكمبيوتر لمكافحة الفيروسات" بصفحة ٤٧).

قد تتلف إعدادات الكمبيوتر نتيجةً لإصابتها ببرمجيات خبيثة أو فشل النظام. قم بتشغيل معالج تحليل الأمان للعثور على أي نقاط اختراق في البرامج المثبتة وأي حيود في إعدادات النظام.

قواعد بيانات التطبيق التي تحتويها حزمة التثبيت قد تصبح قديمة. ابدأ تحديث التطبيق (انظر صفحة ٤٦) (إذا لم يكن قد تم إجراؤه باستخدام معالج التكوين أو تلقائياً فور تثبيت التطبيق).

بعد الانتهاء من إجراءات هذا القسم، سيصبح التطبيق جاهزاً لحماية الكمبيوتر. ولتقييم درجة حماية جهاز الكمبيوتر، استخدم معالج إدارة الأمان (انظر القسم"دارة الأمانإ" بصفحة٥٢).

في هذا القسم:

تحديث التطبيق

تحذير!

يلزم توفير اتصال بالإنترنت لتحديث برنامج مكافحة الفيروسات.

تشتمل مجموعة توزيع التطبيق على قواعد البيانات المحتوية على توقيعات التهديدات. ومع ذلك، فعند تثبيت التطبيق، قد تصبح قواعد البيانات مهملة نظراً لقيام Kaspersky Lab بتحديث قواعد البيانات ووحدات التطبيق بانتظام.

يمكنك تحديد كيفية بدء مهمة التحديث أثناء تشغيل معالج إعداد التطبيق. يقوم برنامج مكافحة الفيروسات من Kaspersky بشكل افتراضي بالبحث عن التحديثات تلقائياً على خوادم تحديث Kaspersky Lab. إذا كان الخادم يحتوي على تحديثات جديدة، سيقوم التطبيق بتحميلها وتثبيتها في الوضع الصامت.

للحفاظ على حماية جهاز الكمبيوتر في حالة محدثة، ننصحك بتحديث برنامج مكافحة الفيروسات من Kaspersky بعد تثبيته مباشرة.

- *للتحديث اليدوي لبرنامج مكافحة الفيروسات من Kaspersky،*

١. افتح نافذة التطبيق الرئيسية.

٢. حدد قسم التحديث في الجانب الأيمن من النافذة.

٣. اضغط زر بدء التحديث.

نتيجة لذلك، سيبدأ تحديث برنامج مكافحة الفيروسات من Kaspersky. ستظهر تفاصيل عملية التحديث في نافذة خاصة.

تحليل الأمان

قد يتلف نظام تشغيل جهاز الكمبيوتر بسبب فشل النظام وبسبب نشاطات البرمجيات الخبيثة. هذا بالإضافة إلى أن تطبيقات المستخدم المثبتة على جهاز الكمبيوتر قد تحتوي على نقاط اختراق تستخدم من قبل الدخلاء لإلحاق أضرار بجهاز الكمبيوتر.

ولاكتشاف مثل هذه المشاكل الأمنية والحد منها، ننصح ببدء معالج محلل الأمان مباشرة بعد إنهاء تثبيت التطبيق. يقوم معالج تحليل الأمان بالبحث عن نقاط الاختراق في التطبيقات المثبتة وعن أي أضرار أو حيود في إعدادات نظام التشغيل والمستعرض.

- *لبدء تشغيل المعالج:*

١. افتح نافذة التطبيق الرئيسية.

٢. في الجزء الأيمن من النافذة، حدد أمان النظام.

٣. ابدأ مهمة محلل الأمان.

فحص الكمبيوتر للبحث عن الفيروسات

يبذل مطورو البرمجيات الخبيثة أقصى ما بوسعهم لإخفاء أنشطة برامجهم، ولذلك فقد لا يلاحظ المستخدم وجود مثل هذه البرمجيات الخبيثة في جهاز الكمبيوتر الخاص به.

بمجرد تثبيت برنامج مكافحة الفيروسات من Kaspersky على جهاز الكمبيوتر، يقوم تلقائياً بإجراء فحص سريع على جهاز الكمبيوتر الخاص بك. تقوم هذه المهمة بالبحث عن البرامج الضارة وإبطال عملها في الكائنات التي يتم تحميلها عند بدء نظام التشغيل.

ويوصي مختصو Kaspersky Lab المستخدم أيضاً بإجراء مهمة فحص كامل.

- *لبدء / إيقاف مهمة فحص الفيروسات:*

١. افتح نافذة التطبيق الرئيسية.

٢. في الجزء الأيمن من النافذة، حدد قسم الفحص (فحص كامل، فحص سريع).

٣. انقر زر بدء الفحص لبدء عملية الفحص. إذا كنت بحاجة إلى إيقاف المهمة، اضغط زر إيقاف الفحص أثناء تقدم عملية الفحص.

إدارة الترخيص

يتطلب برنامج مكافحة الفيروسات من Kaspersky مفتاح ترخيص لكي يعمل. وسيتم تزويدك بمفتاح عند شراء البرنامج. وهو يعطيك حق استخدام البرنامج من يوم الشراء وتثبيت المفتاح.

بدون مفتاح الترخيص، وما لم يتم تفعيل إصدار تجريبي من برنامج مكافحة الفيروسات من Kaspersky، سيتم تشغيل التطبيق في الوضع الذي يسمح بتحديث واحد فقط. ولن يقوم التطبيق بتحميل أي تحديثات جديدة.

إذا تم تفعيل إصدار تجريبي للبرنامج، لن يعمل برنامج مكافحة الفيروسات من Kaspersky بعد انتهاء فترة التجريب.

سيظل البرنامج يعمل عند انتهاء صلاحية مفتاح الترخيص إلا أنك لن تتمكن من تحديث قواعد البيانات. كما كان سابقًا، ستتمكن من فحص جهاز الكمبيوتر الخاص بك للبحث عن فيروسات كما سيمكنك استخدام مكونات الحماية فقط من خلال استخدام قواعد البيانات التي كانت لديك عند انتهاء فترة صلاحية الترخيص. لا نستطيع ضمان حمايتك من الفيروسات التي ستظهر عقب انتهاء صلاحية برنامجك.

لحماية جهاز الكمبيوتر الخاص بك من الإصابة بفيروسات جديدة، نوصي بتجديد مفتاح التطبيق الخاص بك. سيعمل التطبيق على إخطارك قبل انتهاء صلاحية مفتاح التطبيق بأسبوعين. وخلال بعض الأوقات، ستظهر رسالة تفيد بذلك في كل مرة يتم تشغيل التطبيق فيها.

سيتم عرض معلومات عن المفتاح الحالي أسفل **الترخيص** في النافذة الرئيسية لبرنامج مكافحة الفيروسات من Kaspersky: معرف المفتاح ونوعه (تجاري، تجاري باشتراك، تجاري باشتراك حماية، تجريبي، لاختبار بيتا) وعدد الأجهزة المضيفة التي سيتم تثبيت هذا المفتاح عليها وتاريخ انتهاء صلاحية المفتاح وعدد الأيام المتبقية حتى انتهاء الصلاحية. لن يتم عرض المعلومات حول انتهاء المفتاح في حالة تثبيت ترخيص تجاري باشتراك أو ترخيص تجاري باشتراك حماية (انظر القسم "الاشتراك في تجديد الترخيص تلقائياً" بصفحة٤٩).

لعرض نص اتفاقية ترخيص التطبيق، انقر زر **عرض اتفاقية ترخيص المستخدم**. لإزالة مفتاح من القائمة، انقر زر **حذف**.

لشراء أو تجديد مفتاح:

١. شراء مفتاح جديد. للقيام بذلك، استخدم زر **شراء ترخيص** (إذا لم يتم تفعيل التطبيق) أو **تجديد الترخيص**. ستحتوي صفحة الويب التي ستظهر على كافة المعلومات الخاصة بشراء مفتاح من خلال موقع Kaspersky Lab على الإنترنت أو من خلال شركاء الشركة. إذا قمت بالشراء عبر الإنترنت، سيتم إرسال ملف مفتاح أو رمز تفعيل إلى عنوانك المحدد في نموذج أمر الشراء بمجرد الدفع.

٢. تثبيت المفتاح. للقيام بذلك، استخدم زر **تثبيت مفتاح** الموجود في قسم **الترخيص** في نافذة التطبيق الرئيسية أو قم باستخدام أمر **تفعيل** من قائمة التطبيق الرئيسية. This will start the Activation Wizard.

ملاحظة. تقدم Kaspersky Lab بصفة دورية عروض أسعار خاصة لتمديد صلاحية ترخيص منتجاتنا. ابحث عن العروض الخاصة في موقع Kaspersky Lab في قسم **منتجات** ← **مبيعات وعروض خاصة**.

الاشتراك في تجديد الترخيص تلقائياً

عند الحصول على ترخيص من خلال الاشتراك، سيتصل برنامج مكافحة الفيروسات من Kaspersky بخادم التفعيل تلقائياً على فترات زمنية محددة للحفاظ على صلاحية ترخيصك طوال كامل مدة الاشتراك.

وإذا انتهت فترة ترخيص المفتاح الحالي، سيقوم برنامج مكافحة الفيروسات من Kaspersky بالتأكد من وجود مفتاح تم تحديثه على الخادم باستخدام وضع الخلفية وإذا تم العثور على هذا المفتاح، سيقوم التطبيق بتحميله وتثبيته في وضع استبدال المفتاح السابق. وبهذه الطريقة سيتم تجديد الترخيص دون أي تدخل منك. إذا انتهت المدة التي يقوم فيها التطبيق بتجديد الترخيص تلقائيًا، يمكن تجديد الترخيص يدوياً. وأثناء المدة التي يسمح فيها بتجديد الترخيص يدويًا، سيتم الاحتفاظ بوظائف التطبيق. وبعد انقضاء هذه المدة، إذا لم يتم تجديد الترخيص، لن يتم رفع مزيد من تحديثات القواعد (بالنسبة إلى الترخيص التجاري باشتراك)، وكذلك سيتم إيقاف ضمان حماية جهاز الكمبيوتر الخاص بك (بالنسبة إلى الترخيص التجاري باشتراك حماية). لرفض الاشتراك في تجديد الترخيص تلقائيًا، اتصل بموقعنا على الإنترنت الذي قمت بشراء التطبيق منه.

تحذير!

إذا كان برنامج مكافحة الفيروسات من Kaspersky مفعلاً بالفعل باستخدام مفتاح تجاري عند لحظة تفعيل التطبيق، سيتم استبدال هذا المفتاح التجاري بمفتاح اشتراك (مفتاح اشتراك حماية). إذا رغبت في بدء استخدام المفتاح التجاري مجددًا، يجب عليك حذف مفتاح الاشتراك وتفعيل التطبيق مرة أخرى بواسطة رمز التفعيل الذي قمت بالحصول على المفتاح التجاري عن طريق استخدامه سابقًا.

يتصف شرط الاشتراك بالحالات التالية:

١. *تالف*. لم تتم معالجة طلبك لتفعيل الاشتراك بعد (يلزم بعض الوقت لمعالجة الطلب على الخادم). يعمل برنامج مكافحة الفيروسات من Kaspersky في وضع مكتمل الوظائف. إذا لم تتم معالجة طلب الاشتراك بعد فترة زمنية محددة، ستستلم إخطارًا يفيد بعدم معالجة التطبيق. وفي هذه الحالة، لن يتم تحديث قواعد التطبيق بعد ذلك (بالنسبة إلى الترخيص التجاري باشتراك)، وكذلك لن يتم إجراء الحماية لجهاز الكمبيوتر (بالنسبة إلى الترخيص التجاري باشتراك حماية).

٢. *تفعيل*. تم تفعيل الاشتراك في تجديد الترخيص تلقائيًا لمدة غير محددة) لم يتم تحديد التاريخ (أو لفترة زمنية محددة) تم تحديد تاريخ انتهاء الاشتراك).

٣. مجدد. تم تجديد الاشتراك تلقائيًا أو يدويًا لمدة غير محددة) لم يتم تحديد التاريخ (أو لفترة زمنية محددة (تم تحديد تاريخ انتهاء الاشتراك).

٤. *خطأ*: أدى تجديد الاشتراك إلى حدوث خطأ.

٥. *منتهي الصلاحية*. لقد انتهت مدة الاشتراك. يمكنك استخدام رمز تفعيل آخر أو تجديد اشتراكك عن طريق الاتصال بموقعنا على الإنترنت الذي قمت بشراء التطبيق منه..

٦. *إلغاء الاشتراك*. لقد قمت بإلغاء الاشتراك في تجديد الترخيص تلقائيًا.

٧. *يلزم التحديث*. لم يتم استلام مفتاح تجديد الاشتراك في الموعد المحدد لسبب ما. قم باستخدام **تجديد حالة الاشتراك** لتجديد الاشتراك.

بالنسبة إلى الترخيص التجاري باشتراك حماية، يتصف الاشتراك بحالتين إضافيتين:

- متوقف مرحليًا . تم إيقاف الاشتراك في تجديد الترخيص تلقائياً بشكل مرحلي (تاريخ انتهاء صلاحية الاشتراك: تاريخ الإيقاف المرحلي لصلاحية الاشتراك).
- *مستأنف*. تم استئناف الاشتراك في تجديد الترخيص تلقائيًا (تاريخ انتهاء صلاحية الاشتراك غير محدد).

إذا انتهت مدة الاشتراك والمدة الإضافية التي يمكن خلالها تجديد الترخيص) حالة الاشتراك – *منتهي الصلاحية*(، سيخبرك برنامج مكافحة الفيروسات من Kaspersky بذلك وسيتوقف عن محاولاته للحصول على مفتاح محدث من الخادم. بالنسبة إلى الترخيص التجاري باشتراك، سيتم الاحتفاظ بعمل كافة وظائف التطبيق باستثناء خاصية تحديث قواعد التطبيق. بالنسبة إلى الترخيص التجاري باشتراك حماية، لن يتم تحديث قواعد التطبيق وكذلك لن يتم إجراء الحماية لجهاز الكمبيوتر.

إذا لم يتم تجديد الترخيص، لأي سبب، خلال المدة المحددة) حالة التطبيق – *يلزم التحديث*) (على سبيل المثال، إذا كان الكمبيوتر مغلقًا طوال المدة التي كان فيها تجديد الترخيص متاحًا(، يمكنك تجديد الترخيص يدويًا . لهذا الغرض، يمكنك استخدام زر **تجديد حالة الاشتراك**. وحتى يتم تجديد الاشتراك، يتوقف برنامج مكافحة الفيروسات من Kaspersky عن تحديث قواعد بيانات التطبيق (بالنسبة إلى الترخيص التجاري باشتراك)، وكذلك يتوقف عن إجراء الحماية لجهاز الكمبيوتر (بالنسبة إلى الترخيص التجاري باشتراك حماية).

أثناء مدة استخدام الاشتراك، لا يمكنك تثبيت مفاتيح من نوع آخر أو استخدام رمز تفعيل آخر لتجديد الترخيص. ولا يمكنك استخدام رمز تفعيل آخر إلا بعد انتهاء فترة الاشتراك (حالة الاشتراك - *منتهي الصلاحية*).

> تحذير!
>
> الرجاء ملاحظة أنه عند استخدام الاشتراك لتجديد الترخيص تلقائيًا، إذا قمت بإعادة تثبيت التطبيق على جهاز الكمبيوتر الخاص بك، ستحتاج إلى إعادة تفعيل المنتج يدويًا باستخدام رمز التفعيل الذي حصلت عليه عند شراء التطبيق.

المشاركة في شبكة اتصال أمان KASPERSKY

يظهر عدد هائل من التهديدات الجديدة كل يوم على مستوى العالم. لتسهيل عملية جمع إحصائيات حول أنواع التهديدات الجديدة ومصدرها وكيفية التخلص منها، تدعوك Kaspersky Lab إلى استخدام خدمة شبكة اتصال أمان Kaspersky.

يدخل في استخدام شبكة اتصال أمان Kaspersky إرسال المعلومات التالية إلى Kaspersky Lab:

- معرف فريد معين لجهاز الكمبيوتر بواسطة التطبيق. يصف المعرف إعدادات الأجهزة التي بالكمبيوتر ولا يحتوي على أية معلومات أخرى.
- معلومات حول التهديدات المكتشفة بواسطة التطبيق. تتوقف بنية المعلومات ومحتوياتها على نوع التهديد المكتشف.
- معلومات النظام: إصدار نظام التشغيل، حزم الخدمات المثبتة، برامج التشغيل والخدمات القابلة للتحميل، إصدارات برنامج عميل البريد الإلكتروني والمستعرض، ملحقات المستعرض، رقم إصدار برنامج مكافحة الفيروسات من Kaspersky المثبت.

تقوم شبكة اتصال أمان Kaspersky أيضاً بجمع إحصائيات ممتدة، بما في ذلك معلومات عن:

- الملفات القابلة للتنفيذ والتطبيقات الموقعة التي يتم تحميلها على جهاز الكمبيوتر؛
- التطبيقات الجاري تشغيلها على جهاز الكمبيوتر.

يتم إرسال المعلومات الإحصائية بمجرد إتمام تحديث التطبيق.

تحذير!

تضمن Kaspersky Lab ألا يتم القيام بأي جمع أو توزيع للبيانات الشخصية الخاصة بالمستخدم داخل شبكة اتصال أمان Kaspersky.

◄ *لتكوين إرسال الإحصائيات:*

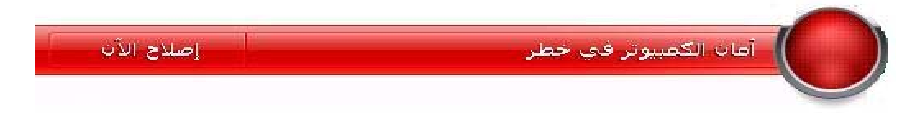
١. افتح نافذة إعداد التطبيق.

٢. حدد قسم المعلومات في الجزء الأيمن من النافذة.

٣. ضع علامة أمام مربع أوافق على المشاركة في شبكة اتصال أمان **Kaspersky** لتأكيد المشاركة في شبكة اتصال أمان Kaspersky. ضع علامة أمام مربع أوافق على إرسال إحصائيات ممتدة ضمن إطار شبكة اتصال أمان **Kaspersky** لتأكيد الموافقة على إرسال إحصائيات ممتدة.

إدارة الأمان

تتم الإشارة إلى وجود مشكلات تتعلق بحماية جهاز الكمبيوتر في نافذة التطبيق الرئيسية عن طريق تغيير لون رمز حالة الحماية ولون اللوحة التي يوجد بها. بمجرد ظهور مشكلة في نظام الحماية، نوصي بالتعامل معها على الفور.



الرسم التوضيحي 5. حالة الحماية الحالية لجهاز الكمبيوتر

يمكنك عرض قائمة بالمشكلات الحالية، ووصفها إلى جانب الحلول الممكنة في علامة التبويب **الحالة** (انظر الرسم التوضيحي التالي) التي يتم فتحها بالنقر على ارتباط إصلاح الآن انظر الرسم التوضيحي السابق).

حالة الحماية - Kaspersky Anti-Virus 2009
Kaspersky Anti-Virus 2009
قواعد البيانات مهملة
الحالة | التهديدات المكتشفة | الإحصائيات
قواعد البيانات مهملة
تم تعطيل الحماية
تم تعطيل حماية جهاز الكمبيوتر. يمكن إصابة المعلومات المخزنة على الكمبيوتر أو تلفها أو الاستيلاء عليها. ينصح بتمكين حماية جهاز الكمبيوتر.
تمكين الحماية
تم تعطيل الدفاع الذاتى
يقوم الدفاع الذاتي بمنع محاولات التطبيقات الأخرى التي تهدف إلى تعديل الملفات ومفاتيح التسجيل التي أنشئت أثناء تثبيت Kaspersky Anti-Virus. الخاصية معطلة الآن ولذا قد يصبح التطبيق غير قابل للتشغيل. ينصح بتمكين الدفاع الذاتي.
تعليمات
إغلاق

الرسم التوضيحي 6. حل مشكلات الأمان

تعرض علامة التبويب قائمة بالمشاكل الحالية. تم إدراج المشاكل على حسب الأهمية كالتالي: أولاً - المشكلات الأكثر خطورة ويظهر الرمز الخاص بها باللون الأحمر، ثانياً - المشكلات الأقل خطورة ويظهر الرمز الخاص بها باللون الأصفر، وتأتي رسائل المعلومات في المرتبة الأخيرة برمزٍ ذي لون أخضر. هناك وصف مفصل لكل مشكلة كما تتوفر الإجراءات التالية:

- الإزالة فوراً. باستخدام الأزرار المقابلة، يمكنك البدء في حل المشكلة، وهو الإجراء الموصى به.

- تأجيل الإزالة. إذا تعذر لأي سبب من الأسباب الإزالة الفورية للمشكلة، يمكنك إرجاء هذا الإجراء والعودة إليه لاحقاً. ولتأجيل الإزالة، استخدم زر إخفاء الرسالة.

  لاحظ أن هذا الخيار لا يتاح مع المشكلات الخطرة. وتتضمن هذه المشكلات على سبيل المثال الكائنات الخبيثة التي تم اكتشافها ولكن لم يتم تنظيفها أو تحطم أحد المكونات أو العديد منها أو تلف ملفات التطبيق.

لإعادة ظهور الرسائل المخفية في القائمة العامة، حدد مربع إظهار الرسائل المخفية.

إيقاف الحماية مؤقتاً

يقصد بإيقاف الحماية مؤقتاً تعطيل كافة مكونات الحماية لفترةٍ زمنية معينة.

▸ *لإيقاف حماية الكمبيوتر مؤقتاً:*

١. حدد عنصر إيقاف الحماية مؤقتاً من قائمة الاختصار بالتطبيق (انظر القسم "قائمة الاختصار" بصفحة ٤٠).

٢. في النافذة التي سوف تفتح، حدد المدة الزمنية التي ترغب في إيقاف الحماية خلالها مؤقتاً:

- في <الفاصل الزمني> - سيتم تمكين الحماية بعد انقضاء هذه المدة الزمنية. استخدم القائمة المنسدلة لتحديد قيمة الفاصل الزمني.

- بعد إعادة التشغيل - سيتم تمكين الحماية بعد إعادة تشغيل النظام، شريطة أن يتم بالفعل تكوين التطبيق بحيث يبدأ عند إعادة تمهيد الكمبيوتر.

- يدوياً - لن تستأنف الحماية إلا بعد بدءها يدوياً. لتمكين الحماية، حدد استئناف الحماية من قائمة الاختصار الخاصة بالتطبيق.

نتيجة لتعطيل الحماية مؤقتاً، سيتم إيقاف كافة مكونات الحماية مؤقتاً. يشار إلى ذلك من خلال:

- الأسماء غير الفعالة (رمادية) للمكونات المعطلة في قسم الحماية بالنافذة الرئيسية.

- رمز التطبيق غير النشط (رمادي اللون) (انظر القسم "رمـز منطقـة الإخطـار" بصفحة ٣٩) في لوحة النظام.
- اللون الأحمر لكل من رمز الحالة ولوحة نافذة التطبيق الرئيسية.

إذا كان قد تم تأسيس اتصالات شبكة اتصال جديدة في نفس الوقت الذي تم فيه إيقاف الحماية مؤقتاً، فسوف يظهر إخطار يشير إلى تعطيلات في هذه الاتصالات.

التحقق من إعدادات التطبيق

بعد تثبيت التطبيق وتكوينه، ينبغي عليك التحقق مما إذا كان تم تكوين التطبيق بشكلٍ صحيحٍ أم لا باستخدام "فيروس" اختبار والتعديلات الخاصة به. ويلزم إجراء اختبار منفصل لكل مكون حماية/بروتوكول.

في هذا القسم:

"فيروس" الاختبار EICAR والتعديلات الخاصة به

تم تصميم "فيروس" الاختبار هذا بمعرفة eicar (المعهد الأوربي لأبحاث مكافحة فيروسات الكمبيوتر) لاختبار منتجات مكافحة الفيروسات على وجه الخصوص.

"فيروس" الاختبار ليس فيروساً في الحقيقة، لعدم احتوائه على رمز يمكن أن يضر بجهاز الكمبيوتر. غير أن معظم جهات تصنيع منتجات مكافحة الفيروسات تطلق على هذا الملف اسم "فيروس".

تحذير!

لا تقم أبداً باستخدام فيروسات حقيقية لاختبار تشغيل أحد منتجات مكافحة الفيروسات!

يمكنك تحميل فيروس الاختبار من موقع الويب الرسمي لمنظمة **EICAR** على العنوان التالي: http://www.eicar.org/anti_virus_test_file.htm.

ملاحظة

قبل تحميل الملف، يجب تعطيل حماية مكافحة الفيروسات على الكمبيوتر لأنك إذا لم تقم بذلك سيقوم التطبيق بتعريف ومعالجة ملف *anti_virus_test_file.htm* على أنه كائن مصاب يتم نقله عبر بروتوكول HTTP.

لا تنس القيام بتمكين حماية مكافحة الفيروسات فور الانتهاء من تحميل "فيروس" الاختبار.

يعرف التطبيق الملفات التي يتم تحميلها من موقع **EICAR** على أنها كائنات مصابة تحتوي على فيروسات يتعذر تنظيفها وعلى ذلك يتخذ إجراءات محددة للتعامل مع مثل هذه الكائنات.

يمكنك أيضاً تعديل "فيروس" الاختبار القياسي للتحقق من فاعلية التطبيق تجاه الأنواع الأخرى من الملفات. ولتعديل "الفيروس"، قم بتغيير محتوى "فيروس" الاختبار القياسي بإضافة أحد البادئات إليه (راجع الجدول أدناه). لإنشاء ملفات "فيروس" معدلة، يمكنك استخدام أي محرر نص أو نص تشعبي، على سبيل المثال **Microsoft Notepad**، **UltraEdit32**، إلخ.

تحذير!

لا يمكن اختبار صحة تشغيل التطبيق باستخدام "فيروس" EICAR المعدل إلا إذا كانت قواعد مكافحة الفيروسات محدثة في 24 أكتوبر 2003 (أكتوبر، 2003 التحديثات التراكمية) أو بعد ذلك.

في الجدول التالي، يحتوي العمود الأول على البادئات التي يجب إضافتها إلى بداية نص "فيروس" القياسي. يدرج العمود الثاني قيم الحالات الممكنة التي يستطيع التطبيق أن يعينها للكائن تبعاً لنتائج الفحص. يشير العمود الثالث إلى كيفية معالجة التطبيق للكائنات ذات الحالة المحددة. الرجاء ملاحظة أن الإجراءات الفعلية المُتخذَة تجاه الكائنات يتم تحديدها من خلال إعدادات التطبيق.

بعد إضافة البادئة إلى "فيروس" الاختبار، احفظ الملف الجديد باسم مختلف، على سبيل المثال: *eicar_dele.com*. قم بتعيين أسماء مشابهة لكافة "الفيروسات" المعدلة.

جدول 6. تعديلات "فيروس" الاختبار

بادئة	حالة الكائن	معلومات معالجة الكائن
فيروس اختبار قياسي بلا بادئة	**مصاب.** كائن يحتوي على رمز فيروس معروف. يتعذر التنظيف.	يتعرف التطبيق على الكائن على أنه فيروس غير قابل للتنظيف. يحدث خطأ عند محاولة تنظيف الكائن؛ سيتم تطبيق الإجراء المقرر اتخاذه مع الكائنات غير القابلة للتنظيف.
CORR–	تالف.	يمكن للتطبيق الوصول إلى الكائن إلا أنه يتعذر عليه فحصه نظراً لتلف الكائن (على سبيل المثال، تلف بنية الملف أو عدم صلاحية تنسيق الملف). يمكن العثور على معلومات حول كيفية معالجة الكائن في التقرير الخاص بتشغيل التطبيق.
WARN–	**مشكوك فيه.** كائن يحتوي على رمز فيروس غير معروف. يتعذر التنظيف.	ثبت أن الكائن مشكوك فيه بواسطة محلل الرمز المساعد على الاكتشاف. وعند الاكتشاف، لم تتضمن قواعد بيانات التطبيق على وصف للإجراء الخاص بمعالجة هذا الكائن. سيتم إخطارك عند اكتشاف أي كائن من هذا النوع.
SUSP–	**مشكوك فيه.** كائن يحتوي على رمز معدل لفيروس معروف. يتعذر التنظيف.	اكتشف التطبيق توافقاً جزئياً لجزء من رمز الكائن مع جزءٍ من رمز فيروس معروف. وعند الاكتشاف، لم تتضمن قواعد بيانات التطبيق على وصف للإجراء الخاص بمعالجة هذا الكائن. سيتم إخطارك عند اكتشاف أي كائن من هذا النوع.
ERRO–	خطأ في الفحص	حدث خطأ أثناء فحص الكائن. تعذر وصول التطبيق للكائن: إما أنه تم اختراق سلامة الكائن (على سبيل المثال، عدم وجود نهاية لأرشيف متعدد الأحجام) أو لا يوجد اتصال إليه (إذا كان موقع الكائن قيد الفحص على قرص شبكة اتصال). يمكنك الحصول على معلومات في تقرير تشغيل التطبيق حول معالجة الكائن.
CURE–	**مصاب.** كائن يحتوي على رمز فيروس معروف. قابل للتنظيف.	يحتوي الكائن على فيروس قابل للتنظيف. سيقوم التطبيق بتنظيف الكائن؛ وسيتم استبدال نص محتوى "الفيروس" بكلمة CURE. سيتم إخطارك عند اكتشاف أي كائن من هذا النوع.

بادئة	حالة الكائن	معلومات معالجة الكائن
DELE–	**مصاب.** كائن يحتوي على رمز فيروس معروف. يتعذر التنظيف.	يتعرف التطبيق على الكائن على أنه فيروس غير قابل للتنظيف. يحدث خطأ عند محاولة تنظيف الكائن؛ سيتم اتخاذ الإجراء المحدد اتخاذه مع الكائنات غير القابلة للتنظيف. سيتم إخطارك عند اكتشاف أي كائن من هذا النوع.

اختبار حماية حركة HTTP

- *للتحقق من أنه تم اكتشاف الفيروسات بنجاح في تدفقات البيانات المرسلة عبر بروتوكول HTTP، الرجاء القيام بما يلي:*

حاول تحميل "فيروس" اختبار من موقع الويب الرسمي لمنظمة **EICAR** على العنوان التالي: http://www.eicar.org/anti_virus_test_file.htm.

عند محاولة تحميل "فيروس" الاختبار، سيقوم برنامج مكافحة الفيروسات من Kaspersky باكتشاف هذا الكائن وتعريفه على أنه كائن مصاب يتعذر تنظيفه، وسيتخذ الإجراء المحدد في إعدادات حركة HTTP لهذا النوع من الكائنات. عند محاولة تحميل "فيروس" الاختبار، سيتم إنهاء الاتصال مع موقع الويب بشكل افتراضي وسيظهر المستعرض رسالة تخبر المستخدم بأن هذا الكائن مصاب بفيروس EICAR-Test-File.

اختبار حماية حركة SMTP

لاكتشاف فيروسات في تدفقات البيانات المرسلة باستخدام بروتوكول SMTP، يجب عليك استخدام نظام بريد إلكتروني يستخدم هذا البروتوكول لنقل البيانات.

> ملاحظة
>
> نوصيك باختبار كيفية تعامل برنامج مكافحة الفيروسات من Kaspersky مع رسائل البريد الإلكتروني الواردة والصادرة بما في ذلك نص الرسالة والمرفقات. لاختبار اكتشاف الفيروسات في نص الرسائل، قم بنسخ نص "فيروس" الاختبار القياسي أو "الفيروس" المعدل إلى نص الرسالة.

◀ *لاختبار اكتشاف فيروسات في تدفقات بيانات SMTP:*

١. أنشئ رسالة بتنسيق نص عادي باستخدام عميل بريد إلكتروني مثبت على جهاز الكمبيوتر.

ملاحظة
لن يتم فحص أية رسالة تحتوي على فيروس اختبار إذا تم إنشاؤها بتنسيق RTF أو HTML!

٢. انسخ نص "فيروس" الاختبار القياسي أو المعدل في بداية الرسالة أو أرفق بالرسالة ملفاً يحتوي على "فيروس" الاختبار.

٣. أرسل الرسالة إلى مسئول النظام.

سوف يكتشف التطبيق الكائن ويعرفه على أنه مصاب ويمنع الرسالة.

التحقق من إعدادات مكافحة فيروسات الملفات

◀ *للتحقق من صحة تكوين مكون مكافحة فيروسات الملفات، الرجاء القيام بما يلي:*

١. قم بإنشاء مجلدٍ على أحد الأقراص وانسخ فيه "فيروس" الاختبار الذي قمت بتحميله، و"فيروسات" الاختبار المعدلة التي قمت بإنشائها.

٢. تأكد من تسجيل جميع الأحداث بحيث يحتفظ ملف التقرير ببيانات حول الكائنات التالفة والكائنات التي لم يتم فحصها لاحتوائها على أخطاء.

٣. قم بتشغيل "فيروس" الاختبار أو نسخة معدلة منه.

سيعترض مكون مكافحة فيروسات الملفات استدعاء الملف، وسيقوم بفحصه واتخاذ الإجراء المحدد في الإعدادات الخاصة بالكائنات المشابهة. وعند تحديد إجراءات مختلفة ليتم اتخاذها حيال الكائن المكتشف، يمكنك إجراء فحص كامل لتشغيل المكون.

يمكنك استعراض معلومات حول نتائج تشغيل مكون مكافحة فيروسات الملفات في التقرير الخاص بتشغيل المكون.

التحقق من إعدادات مهمة فحص الفيروسات

للتحقق من صحة تكوين مهمة فحص مكافحة الفيروسات، الرجاء القيام بما يلي:

١. قم بإنشاء مجلدٍ على أحد الأقراص وانسخ فيه "فيروس" الاختبار الذي قمت بتحميله، و"فيروسات" الاختبار المعدلة التي قمت بإنشائها.

٢. قم بإنشاء مهمة جديدة لفحص الفيروسات وحدد المجلد الذي يحتوي على مجموعة "فيروسات" الاختبار، بوصفه الكائن المطلوب فحصه.

٣. تأكد من تسجيل جميع الأحداث بحيث يحتفظ ملف التقرير ببيانات حول الكائنات التالفة والكائنات التي لم يتم فحصها لاحتوائها على أخطاء.

٤. قم بتشغيل مهمة فحص الفيروسات.

عندما تكون مهمة الفحص قيد التشغيل، سيتم القيام بالإجراءات المحددة في تكوين المهمة التي يتم تنفيذها في حالة اكتشاف كائنات مشكوك فيها أو مصابة. عند تحديد إجراءات متنوعة ليتم تنفيذها حيال كائنات تم اكتشافها، سوف تتمكن من إجراء فحص كامل لتشغيل المكون.

يمكنك استعراض المعلومات التفصيلية حول إجراءات المهمة في التقرير الخاص بتشغيل المكون.

بيان تجميع بيانات شبكة أمان
KASPERSKY

مقدمة

الرجاء قراءة هذه الوثيقة بعناية. فهي تحتوي على معلومات هامة ينبغي عليك الإلمام بها قبل مواصلة استخدام خدماتنا أو برامجنا. تعتبر مواصلة استخدام برامج وخدمات شركة KASPERSKY LAB قبولاً منك ببيان تجميع البيانات هذا الخاص بشركة KASPERSKY LAB. ونحتفظ بالحق في تعديل بيان تجميع البيانات هذا في أي وقت عن طريق نشر التغييرات في هذه الصفحة. الرجاء التحقق من تاريخ المراجعة أدناه لتحدد ما إذا كانت هناك تعديلات قد أجريت على الوثيقة منذ آخر مرة قمت بالاطلاع عليها أم لا. إن مواصلة استخدامك لأي جزء من خدمات Kaspersky Lab عقب إعلان تحديث بيان تجميع البيانات يمثل قبولاً منك بالتغييرات الواردة فيه.

قامت شركة Kaspersky Lab والمؤسسات التابعة لها (والتي يشار إليها إجمالاً بعبارة "***Kaspersky Lab***") بإعداد بيان تجميع البيانات هذا بغرض الإفصاح والإخبار عن ممارسات تجميع البيانات ونشرها الخاصة بها لبرامج مكافحة الفيروسات وأمان الإنترنت من Kaspersky.

كلمة من شركة Kaspersky Lab

تلتزم شركة Kaspersky Lab التزاماً راسخاً بتقديم خدمة فائقة الجودة لكافة عملائها وخاصة فيما يتعلق بقلقهم حيال تجميع البيانات. إننا نتفهم أنه يحق أن تكون لديكم تساؤلات حول كيفية قيام شبكة اتصال أمان Kaspersky بجمع واستخدام المعلومات والبيانات، لذا فقد أعددنا هذا البيان لإخباركم بقواعد تجميع البيانات التي تحكم شبكة اتصال أمان Kaspersky ("بيان تجميع البيانات" أو "البيان").

يحتوي بيان تجميع البيانات هذا على العديد من التفاصيل العامة والفنية حول الخطوات التي نتخذها لمراعاة مخاوفكم بشأن تجميع البيانات. لقد أعددنا بيان تجميع البيانات هذا حسب عمليات ومناطق رئيسية حتى يمكنك أن تستعرض سريعاً المعلومات التي تهمك. إن الأساس الذي نعمل وفقه هو أن تلبية احتياجاتك وتوقعاتك تشكل قاعدة لكل ما نقوم به - بما في ذلك حماية تجميع بياناتك.

يتم جمع البيانات والمعلومات بمعرفة شركة Kaspersky Lab، وإذا راودتك أي تساؤلات أو مخاوف بشأن تجميع البيانات بعد استعراض بيان تجميع البيانات هذا، الرجاء إرسال بريد إلكتروني على العنوان التالي: support@kaspersky.com.

ما هي شبكة اتصال أمان Kaspersky؟

تتيح خدمة شبكة اتصال أمان Kaspersky لمستخدمي منتجات أمان Kaspersky Lab من جميع أرجاء العالم إمكانية المساعدة على تسهيل عملية التعريف وخفض المدة التي تستغرقها في تقديم الحماية ضد المخاطر الأمنية الجديدة ("في حالتها الطبيعية") التي تستهدف جهاز الكمبيوتر. ولتحديد التهديدات الجديدة ومصادرها والعمل على تحسين حالة أمان المستخدم وكفاءة أداء المنتج، تقوم شبكة اتصال أمان Kaspersky بجمع بيانات التطبيق

والأمان المحددة حول المخاطر الأمنية المحتملة والتي تستهدف جهاز الكمبيوتر ثم تقديم هذه البيانات إلى Kaspersky Lab لإجراء التحليل. ولا تحتوي هذه المعلومات على معلومات يمكن استخدامها في التعرف على شخص المستخدم ولا تستخدمها شركة **Kaspersky Lab** إلا بغرض تعزيز منتجات الأمان الخاصة بها ودعم تطور الحلول ضد التهديدات والفيروسات الخبيثة. في حالة إرسال أي بيانات شخصية عن المستخدم على نحو غير مقصود، تقوم **Kaspersky Lab** بحفظها وحمايتها طبقاً لبيان تجميع البيانات هذا.

تسهم مشاركتك أنت وغيرك من مستخدمي منتجات الأمان من Kaspersky Lab من جميع أرجاء العالم في شبكة اتصال أمان Kaspersky إسهاماً كبيراً في توفير بيئة إنترنت أكثر أماناً.

المسائل القانونية

تخضع شبكة اتصال أمان Kaspersky لقوانين العديد من السلطات القضائية نظرًا لاستخدام خدماتها في نطاق سلطات قضائية مختلفة، بما في ذلك الولايات المتحدة الأمريكية. ينبغي أن تكشف شركة Kaspersky Lab عن معلومات تعريف الشخصية دون الحصول على تصريح من المستخدم في حالة مطالبة القانون بذلك أو عند الاعتقاد عن نية حسنة بأن اتخاذ مثل هذا الإجراء يعد أمرًا ضروريًا للتحقق من أو الحماية ضد الأنشطة الضارة بضيوف Kaspersky Lab أو زائريها أو شركائها أو بملكيتها أو ضد الأنشطة الضارة بآخرين. كما هو مذكور أعلاه، تختلف القوانين المتعلقة بالبيانات والمعلومات التي تجمعها شبكة اتصال أمان Kaspersky من دولة إلى أخرى. على سبيل المثال، تخضع بعض المعلومات التي يمكن استخدامها في التعرف على شخص المستخدم والتي تم جمعها في الاتحاد الأوروبي والدول الأعضاء به إلى توجيهات الاتحاد الأوروبي المتعلقة بالبيانات الشخصية والخصوصية والاتصالات الإلكترونية، بما في ذلك، على سبيل المثال لا الحصر، التوجيه رقم EC/58/2002 الصادر عن البرلمان الأوروبي وعن المجلس المنعقد في الثاني عشر من يوليو 2002 فيما يخص معالجة البيانات الشخصية وحماية الخصوصية في قطاع الاتصالات الإلكترونية والتوجيه رقم EC/46/95 الصادر عن البرلمان الأوروبي والمجلس المنعقد في الرابع والعشرين من أكتوبر 1995 بشأن حماية الأفراد فيما يتعلق بمعالجة البيانات الشخصية وكذلك حول الانتقال الحر لهذه البيانات والتشريع اللاحق الذي أقرته الدول الأعضاء بالاتحاد الأوروبي، واعتمده قرار المفوضية الأوروبية رقم EC/2001/497 حول البنود التعاقدية القياسية (البيانات الشخصية المرسلة إلى دول العالم الثالث) والتشريع اللاحق الذي أقرته الدول الأعضاء بالمفوضية الأوروبية.

يتعين على شبكة اتصال أمان Kaspersky إبلاغ المستخدمين المعنيين كما ينبغي، في المرحلة الأولى لجمع المعلومات المذكورة أعلاه، بأي مشاركة لهذه المعلومات، وبالأخص فيما يتعلق بالاستخدام لغرض تطوير الأعمال، وتسمح الشبكة لمستخدمي الإنترنت هؤلاء باختيار إما المشاركة (في الدول الأعضاء بالمفوضية الأوروبية والدول الأخرى التي تتطلب إجراء المشاركة) أو بعدم المشاركة (بالنسبة إلى كافة الدول الأخرى) من خلال الإنترنت في الاستخدام التجاري لهذه البيانات و/أو إرسال هذه البيانات إلى أطراف ثالثة.

ويجوز أن يُطلب من Kaspersky Lab بحكم القانون أو من قبل الجهات القضائية تقديم بعض المعلومات التي يمكن استخدامها في التعرف على شخص المستخدم إلى الجهات الحكومية المختصة. وفي حالة طلب هذه المعلومات بحكم القانون أو من قبل الجهات القضائية، فإننا نلتزم بتقديمها فور استلام الوثيقة المناسبة. كما يجوز لشركة Kaspersky Lab أيضاً تقديم معلومات إلى الجهات المختصة بتنفيذ القانون لحماية ممتلكاتها وصيانة صحة وسلامة الأفراد حسبما يسمح به القانون.

يتعين تقديم إعلان إلى سلطات الدول الأعضاء في قانون حماية البيانات الشخصية وفقاً للتشريع اللاحق المعمول به في الدول الأعضاء بالاتحاد الأوروبي. ويتعين إتاحة الوصول إلى المعلومات الخاصة بتلك الإعلانات على خدمات شبكة اتصال أمان Kaspersky.

معلومات مجمعة

البيانات التي نجمعها

تقوم خدمة شبكة اتصال أمان Kaspersky بجمع وتقديم بيانات أساسية وموسعة إلى Kaspersky Lab حول المخاطر الأمنية المحتملة التي تستهدف جهاز الكمبيوتر. تتضمن البيانات التي يتم جمعها:

البيانات الأساسية

- معلومات عن أجهزة وبرامج الكمبيوتر، بما في ذلك نظام التشغيل وحزم الخدمات المثبتة، كائنات النواة، برامج التشغيل، الخدمات، ملحقات Internet Explorer، ملحقات الطباعة، ملحقات Windows Explorer، ملفات البرامج التي تم تحميلها، عناصر الإعداد النشطة، التطبيقات الصغيرة للوحة التحكم، السجلات المضيفة وسجلات التسجيل، عناوين IP، أنواع المستعرضات، عملاء البريد الإلكتروني، رقم إصدار منتج Kaspersky Lab، والتي لا تعد عادة معلومات يمكن استخدامها في التعرف على شخص المستخدم؛

- معرف فريد يتم إنشاؤه بواسطة منتج Kaspersky Lab لتعريف الأجهزة الشخصية دون تعريف المستخدم وهو لا يتضمن أي معلومات شخصية.

- معلومات حول حالة حماية جهاز الكمبيوتر ضد الفيروسات، وبيانات حول أي ملفات أو أنشطة يشتبه في كونها برمجيات خبيثة (على سبيل المثال، اسم الفيروس، تاريخ/وقت الاكتشاف، أسماء/مسارات وحجم الملفات المصابة، عنوان IP ومنفذ هجوم شبكة الاتصال، اسم التطبيق الذي يشتبه في كونه برنامجاً خبيثاً). الرجاء ملاحظة أن البيانات المجمعة المشار إليها أعلاه لا تحتوي على أي معلومات يمكن استخدامها في التعرف على شخص المستخدم.

بيانات موسعة

- معلومات حول التطبيقات الموقعة رقمياً والتي يتم تحميلها بواسطة المستخدم (محدد موقع المعلومات (URL)، حجم الملف، اسم المُوقع)

- معلومات حول التطبيقات القابلة للتنفيذ (الحجم، السمات، تاريخ الإنشاء، معلومات حول رؤوس PE، المنطقة، الاسم، المَوقع، أداة الضغط المستخدمة).

تأمين إرسال وتخزين البيانات

تلتزم Kaspersky Lab بحماية أمان المعلومات التي تجمعها. يتم تخزين البيانات التي تم جمعها في خوادم الكمبيوتر مع تحديد وتقييد إمكانية الوصول. تشغل Kaspersky Lab شبكات اتصال بيانات آمنة ومحمية بجدار حماية يخضع لمعايير الصناعة وبأنظمة كلمة المرور. تستخدم Kaspersky Lab نطاقاً عريضاً من إجراءات وتقنيات الأمان لحماية المعلومات التي يتم جمعها من التهديدات مثل الوصول أو الاستخدام أو الكشف غير المصرح به. تتم مراجعة وتعزيز سياسات الأمان الخاصة بنا بصفة دورية حسبما تقتضيه الضرورة، ولا يسمح بالوصول إلى البيانات التي نجمعها إلا للأفراد المصرح لهم فحسب. تتخذ Kaspersky Lab الخطوات اللازمة لضمان أمان التعامل مع معلوماتك ووفقاً لهذا البيان. وللأسف، لا يمكن ضمان أمان أي من عمليات إرسال البيانات. ونتيجة لذلك، وبينما نبذل أقصى ما في وسعنا لحماية بياناتك، لا يمكن أن نضمن أمان أي بيانات ترسلها إلينا أو تنقلها من

منتجاتنا أو خدماتنا، بما في ذلك على سبيل المثال لا الحصر شبكة اتصال أمان Kaspersky، وتقوم باستخدام كافة هذه الخدمات على مسؤوليتك الشخصية.

يجوز إرسال البيانات التي يتم جمعها إلى خوادم Kaspersky Lab، وقد اتخذت Kaspersky Lab الاحتياطات اللازمة لضمان تمتع البيانات المجمعة، في حالة إرسالها، بمستوى مناسب من الحماية. إننا نتعامل مع البيانات التي نجمعها على أنها معلومات سرية، وعلى هذا الأساس فهي تخضع لإجراءات الأمان الخاصة بنا ولسياسات الشركة المعنية بحماية واستخدام المعلومات السرية. وبعد وصول البيانات المجمعة إلى Kaspersky Lab، يتم تخزينها على خادم يتميز بخصائص أمان مادية وإلكترونية حسبما هو متعارف عليه في الصناعة، بما في ذلك استخدام إجراءات تسجيل الدخول/كلمة المرور وجدران الحماية الإلكترونية المصممة لمنع الوصول غير المصرح به من خارج Kaspersky Lab. تتم معالجة وتخزين البيانات المجمعة بمعرفة شبكة اتصال أمان Kaspersky والتي يتناولها هذا البيان، في الولايات المتحدة وربما في نطاق سلطات قضائية أخرى وكذلك في دول أخرى تدير فيها Kaspersky Lab أعمالها. جميع موظفي Kaspersky Lab على دراية بسياسات الأمان الخاصة بنا. ولا يستطيع أحد الوصول إلى بياناتك سوى أولئك الموظفين الذين يحتاجونها بغرض القيام بوظائفهم. لن يتم ربط أي بيانات مخزنة بأي معلومات تعريف الشخصية. لا تقوم شركة Kaspersky Lab بدمج البيانات المخزنة بواسطة شبكة اتصال أمان Kaspersky مع أي بيانات أو قوائم اتصال أو معلومات اشتراك والتي تجمعها Kaspersky Lab لأغراض ترويجية أو غيرها.

استخدام البيانات المجمعة

كيفية استخدام بياناتك الشخصية

تجمع Kaspersky Lab البيانات بغرض تحليل وتعريف مصدر المخاطر الأمنية المحتملة، ولتحسين قدرة منتجات Kaspersky Lab على اكتشاف الأنشطة الخبيثة والمواقع الاحتيالية وبرمجيات الجرائم وأنواع أخرى من تهديدات أمان الإنترنت وذلك بغرض توفير أفضل مستوى ممكن من الحماية لعملاء Kaspersky Lab في المستقبل.

كشف المعلومات إلى أطراف ثالثة

يجوز لشركة Kaspersky Lab الكشف عن أي معلومات تم جمعها إذا طلب منها أحد مسئولي تنفيذ القانون ذلك حسبما يقتضيه أو يسمح به القانون أو استجابة لأمر قضائي للمثول أمام المحكمة أو أي أمر قانوني آخر أو إذا اعتقدنا بنية حسنة أننا مطالبون بالقيام بذلك التزاما بالقانون المعمول به أو اللائحة التنظيمية أو أمر قضائي للمثول أمام المحكمة أو أمر قانوني آخر أو طلب حكومي قابل للنفاذ. ويجوز أن تكشف Kaspersky Lab أيضاً عن معلومات تعريف الشخصية عندما يتوافر لدينا سبب يجعلنا نرى بضرورة كشف هذه المعلومات لتعريف أو الاتصال أو اتخاذ إجراء قانوني ضد أي شخص قد ينتهك هذا البيان أو بنود الاتفاقيات التي تبرمها مع الشركة أو لحماية سلامة مستخدمينا وحماية العامة أو بموجب اتفاقيات الترخيص والخصوصية مع أطراف ثالثة معينة والتي قد تساعدنا في تطوير وتشغيل وصيانة شبكة اتصال أمان Kaspersky. يجوز أن تشارك Kaspersky Lab بمعلومات معينة مع منظمات البحث وجهات بيع برامج الأمان الأخرى بغرض زيادة الوعي واكتشاف ومنع مخاطر الإنترنت الأمنية. يجوز أن تستفيد Kaspersky Lab أيضاً من الإحصائيات المشتقة من المعلومات المجمعة لتتبع ونشر تقارير بشأن اتجاهات المخاطر الأمنية.

الاختيارات المتاحة لك

المشاركة اختيارية في شبكة اتصال أمان Kaspersky. ويمكنك تفعيل وإلغاء تفعيل خدمة شبكة اتصال أمان Kaspersky في أي وقت من خلال زيارة إعدادات المعلومات تحت صفحة خيارات منتج Kaspersky Lab. ولكن الرجاء ملاحظة أنه إذا كان ينبغي عليك اختيار الامتناع عن تقديم المعلومات أو البيانات المطلوبة، فقد يتعذر علينا تزويدك ببعض الخدمات التي تعتمد على جمع هذه البيانات.

وبمجرد انتهاء فترة خدمة منتج Kaspersky Lab، قد يستمر عمل بعض وظائف برنامج Kaspersky Lab، ولكن سيتوقف إرسال المعلومات تلقائياً إلى Kaspersky Lab بعد ذلك.

ويحق لنا أيضاً إرسال رسائل تنبيه على فترات متباعدة إلى المستخدمين لإبلاغهم ببعض التغييرات المعينة التي قد تؤثر على قدرتهم على استخدام خدماتنا التي قاموا بالتسجيل فيها مسبقاً. كما يحق لنا الاتصال بك إذا اضطررنا لذلك كجزء من إجراء قانوني أو إذا كان ثمة انتهاك لأي اتفاقيات ترخيص وضمان وشراء سارية المفعول.

تحتفظ Kaspersky Lab بهذه الحقوق لأننا نشعر في حالات محدودة أننا قد نحتاج إلى حق الاتصال بك كإجراء قانوني أو بشأن مسائل قد تكون هامة بالنسبة لك. ولا تسمح لنا هذه الحقوق بالاتصال بك لتسويق خدمات جديدة أو قائمة إذا طلبت منا عدم القيام بذلك، ويعد إجراء هذا النوع من الاتصالات أمراً نادراً.

جمع البيانات - تساؤلات وشكاوى ذات صلة

تراعي Kaspersky Lab مخاوف المستخدمين المتعلقة بجمع البيانات وتتعامل معها بفائق الاحترام والعناية. إذا اعتقدت أن هناك حالة من عدم الالتزام بهذا البيان فيما يتعلق بمعلوماتك أو بياناتك أو كانت لديك تساؤلات أو مخاوف أخرى ذات صلة، يمكنك مراسلتنا أو الاتصال بشركة Kaspersky Lab من خلال البريد الإلكتروني التالي: support@kaspersky.com.

الرجاء أن تصف في رسالتك طبيعة تساؤلك بأكبر قدر ممكن من التفصيل. سوف نحقق في تساؤلك أو شكواك دون إبطاء.

يعد تقديم المعلومات أمراً اختيارياً. يمكن تعطيل خيار جمع البيانات بواسطة المستخدم في أي وقت في قسم "المعلومات" في صفحة "الإعدادات" بأي منتج ملائم من منتجات Kaspersky.

KASPERSKY LAB

تأسست شركة Kaspersky Lab عام 1997 وأصبحت رائداً معترفاً به في تقنيات أمان المعلومات. فهي تنتج تشكيلة عريضة من برامج حماية البيانات التي تتميز بالأداء العالي، بما في ذلك أنظمة مكافحة الفيروسات ومكافحة البريد الإلكتروني غير المرغوب فيه ومكافحة القرصنة.

إن شركة Kaspersky Lab شركة عالمية. ومقرها الرئيسي في روسيا، ولديها فروع في المملكة المتحدة وفرنسا وألمانيا واليابان ودول البينلوكس (بلجيكا ولكسمبورج وهولندا) والصين وبولندا ورومانيا والولايات المتحدة الأمريكية (ولاية كاليفورنيا). وتأسس حديثاً في فرنسا، مقراً جديداً للشركة، وهو مركز البحث الأوروبي المعني ببرامج مكافحة الفيروسات. وتضم شبكة شركاء Kaspersky أكثر من 500 شركة على مستوى العالم.

وتوظف شركة Kaspersky حالياً أكثر من 450 خبيراً محترفاً، من بينهم 10 خبراء حاصلين على درجة الماجستير في إدارة الأعمال و16 خبيراً حاصلين على درجة الدكتوراة. ويحمل العديد من كبار خبراء شركة Kaspersky Lab عضوية منظمة الباحثين المعنيين بمكافحة فيروسات الكمبيوتر.

ويعد أقيم أصل لشركتنا هو المعرفة الفريدة وخبرات خبرائها المتراكمة على مدار أربعة عشر عاماً في محاربة فيروسات الكمبيوتر على نحوٍ متواصل. ويُمَكن التحليل الشامل لأنشطة فيروسات الكمبيوتر متخصصي الشركة من توقع اتجاهات تطوير البرمجيات الخبيثة، وتوفير حماية دائمة للمستخدم ضد أنواع الهجمات الجديدة. تعد مقاومة الهجمات المستقبلية السياسة الأساسية المتبعة في كافة منتجات Kaspersky Lab. وفي جميع الأوقات، تتفوق منتجات الشركة على الشركات الأخرى في تقديم تغطية لبرامج مكافحة الفيروسات لعملائنا.

وقد ساهمت سنوات العمل الشاق في جعل الشركة واحدة من كبار مطوري برامج مكافحة الفيروسات. وكانت شركة Kaspersky Lab واحدة من أوائل الشركات التي قامت بتطوير العديد من معايير برامج مكافحة الفيروسات الحديثة. ويقدم المنتج الأساسي للشركة، Kaspersky Anti-Virus، حماية كاملة لجميع طبقات شبكة الاتصال: ومحطات العمل وخوادم الملفات ونظم البريد الإلكتروني وجدران الحماية وبوابات الإنترنت وأجهزة الكمبيوتر اليدوية. وتوفر أدوات الإدارة الملائمة وسهلة الاستخدام أقصى درجات الحماية الآلية لبرامج مكافحة الفيروسات في أجهزة الكمبيوتر وشبكات اتصال الشركات. وتستخدم الكثير من شركات تصنيع البرامج ذائعة الصيت نواة برنامج مكافحة الفيروسات من Kaspersky في منتجاتهم؛ من بين هذه الشركات شركة Nokia ICG (الولايات المتحدة الأمريكية)، و F-Secure (فنلندا)، و Aladdin (إسرائيل)، و Sybari (الولايات المتحدة الأمريكية)، و G Data (ألمانيا)، و Deerfield (الولايات المتحدة الأمريكية)، و Alt-N (الولايات المتحدة الأمريكية)، و Microworld (الهند)، و BorderWare (كندا).

ويتمتع عملاء شركة Kaspersky Lab بكمٍ كبير من الخدمات الإضافية التي تضمن استقرار تشغيل منتجات الشركة والتوافق مع متطلبات النشاط التجاري الخاصة بالعملاء. فنحن نصمم وننفذ وندعم مجموعات مركبة من برامج مكافحة الفيروسات للشركات. ويتم تحديث قاعدة بيانات مكافحة الفيروسات لشركة Kaspersky Lab كل ساعة. وتقدم الشركة لعملائها خدمة الدعم الفني على مدار 24 ساعة متاحة بعدة لغات.

إذا كانت لديك أي استفسارات، يمكنك الاتصال بوكلائنا أو الاتصال بشركة Kaspersky Lab مباشرة. ويتم تقديم استشارات تفصيلية عبر الهاتف أو البريد الإلكتروني. وسوف تجد إجابات شاملة وكاملة عن أي سؤال تطرحه.

العنوان:	Russia, 123060, Moscow, 1-st Volokolamsky Proezd, 10, Building 1
التليفون والفاكس:	٧٩٧-٨٧-٠٠ (٤٩٥) ٧+، ٦٤٥-٧٩-٣٩ (٤٩٥) ٧+، ٩٥٦-٧٠-٠٠ (٤٩٥) ٧+
دعم للطوارئ على مدار أربع وعشرين ساعة طوال أيام الأسبوع.	٧٩٧-٨٧-٠٧ (٤٩٥) ٧+، ٦٤٥-٧٩-٢٩ (٤٩٥) ٧+، ٩٥٦-٨٧-٠٨ (٤٩٥) ٧+
دعم مستخدمي المنتج الموجه للأعمال التجارية:	٧٩٧-٨٧-٠٧ (٤٩٥) ٧+، ٦٤٥-٧٩-٢٩ (٤٩٥) ٧+، ٩٥٦-٨٧-٠٨ (٤٩٥) ٧+ (من العاشرة صباحاً وحتى السابعة مساءً) http://support.kaspersky.com/helpdesk.html
دعم مستخدمي الشركات:	سيتم تقديم بيانات الاتصال بعد شراء برنامج مخصص للشركات وفقاً للحزمة المدعومة الخاصة بك.
منتدى ويب Kaspersky Lab:	http://forum.kaspersky.com
معمل مكافحة الفيروسات:	newvirus@kaspersky.com (مخصص فقط لإرسال الفيروسات الجديدة في الأرشفة)
المجموعة المعنية بإنشاء وثائق المستخدم:	docfeedback@kaspersky.com (مخصص فقط لإرسال ملاحظات بشأن الوثائق ونظام التعليمات)
إدارة المبيعات:	٧٩٧-٨٧-٠٠ (٤٩٥) ٧+، ٦٤٥-٧٩-٣٩ (٤٩٥) ٧+، ٩٥٦-٧٠-٠٠ (٤٩٥) ٧+ sales@kaspersky.com
معلومات عامة:	٧٩٧-٨٧-٠٠ (٤٩٥) ٧+، ٦٤٥-٧٩-٣٩ (٤٩٥) ٧+، ٩٥٦-٧٠-٠٠ (٤٩٥) ٧+ info@kaspersky.com

:WWW	http://www.kaspersky.com/ http://www.viruslist.com

CRYPTOEX LLC

لإنشاء توقيعات رقمية والتحقق منها، يعمل برنامج مكافحة الفيروسات من Kaspersky على استخدام مكتبة برنامج أمان البيانات Crypto C من Crypto Ex LLC.

تحمل شركة Crypto Ex ترخيص الوكالة الفيدرالية للاتصالات والمعلومات الحكومية (إحدى فروع خدمة الحماية الفيدرالية) لتطوير وتصنيع وتوزيع برامج تشفير لحماية البيانات التي لا تعتبر سراً من أسرار الدولة.

تم تصميم مكتبة Crypto C لحماية المعلومات السرية من فئة KS1، وقد منحت شهادة الامتثال من خدمة الأمن الفيدرالي رقم SF/114-0901 بتاريخ 1 يوليو 2006.

تقوم المكتبة بتشفير وفك تشفير حزم البيانات ذات الحجم الثابت و/أو تدفقات البيانات باستخدام التقنيات التالية:

- خوارزمية تشفير (GOST 28147-89)؛ و
- خوارزميات لتوليد والتحقق من التوقيعات الإلكترونية الرقمية وفقاً للخوارزميات (GOST R 34.10-94 و GOST 34.10-2001)؛ و
- دوال التجزئة (GOST 34.11-94)؛ و
- توليد معلومات المفتاح باستخدام ناقل برنامج الرقم العشوائي الزائف؛ و
- معلومات مفتاح ونظام إنشاء موجه محاكاة (GOST 28147-89).

تم تنفيذ الوحدات النمطية للمكتبة باستخدام ANSI C، ويمكن دمجها في التطبيقات كرمز تم تحميله بطريقة ثابتة أو متغيرة. ويمكن تنفيذها على مجموعة متنوعة من الأنظمة الأساسية بما في ذلك x86، x86-64، Ultra SPARC II والأنظمة الأساسية المتوافقة.

يمكن نقل الوحدات النمطية للمكتبة إلى بيئات التشغيل التالية: Microsoft Windows NT/XP/98/2000/2003، Unix (Linux، FreeBSD، SCO Open Unix 8.0، SUN Solaris، SUN Solaris الخاصة بـ Ultra SPARC II).

للمزيد من المعلومات، الرجاء زيارة موقع شركة CryptoEx LLC على http://www.cryptoex.ru، أو الاتصال بالشركة عن طريق البريد الإلكتروني علي info@cryptoex.ru.

مؤسسة MOZILLA

تم استخدام إصدار library **Gecko SDK ver. 1.8** لتطوير مكونات هذا التطبيق.

لمزيد من التفاصيل حول مكتبة **Gecko SDK** الرجاء الرجوع إلى:
http://developer.mozilla.org/en/docs/Gecko_SDK.

موقع ويب مؤسسة Mozilla: http://www.mozilla.org.

اتفاقية الترخيص

اتفاقية ترخيص المستخدم النهائي القياسية

إخطار إلى جميع المستخدمين: اقرأ بعناية الاتفاقية القانونية التالية المشار إليها باسم ("الاتفاقية")، التي تتعلق بترخيص برنامج مكافحة الفيروسات من KASPERSKY المشار إليه باسم ("البرنامج") الذي تنتجه شركة KASPERSKY LAB المشار إليها باسم ("KASPERSKY LAB").

إذا اشتريت هذا البرنامج عبر الإنترنت بالنقر على زر أوافق، فإنك (سواءً أكنت فرداً أم كياناً مستقلاً) توافق على الالتزام بهذه الاتفاقية وعلى أن تصبح طرفاً فيها. وإذا لم توافق على جميع بنود هذه الاتفاقية، انقر على الزر الذي يشير إلى عدم قبولك لبنود هذه الاتفاقية ولا تقم بتثبيت البرنامج.

إذا اشتريت هذا البرنامج على وسيطٍ مادي، فإن قيامك بفض غلاف القرص المدمج (سواءً أكنت فرداً أم كياناً مستقلاً) يعني موافقتك على الالتزام بهذه الاتفاقية. وإذا لم توافق على جميع بنود هذه الاتفاقية، لا تقم بفض غلاف القرص المدمج أو تحميل هذا البرنامج أو تثبيته أو استخدامه.

وطبقاً لما ينص عليه التشريع، وفيما يتعلق بشراء برنامج KASPERSKY الذي يهدف إلى خدمة العملاء الأفراد عبر الإنترنت من موقع الويب الخاص بشركة KASPERSKY LAB أو أحد شركائها، يكون للعميل مهلة تصل إلى أربعة عشر يوماً (14) من أيام العمل اعتباراً من تاريخ تسلم المنتج، لإعادته إلى البائع لاستبداله بآخر أو استرداد قيمته، بشرط عدم فض ختم البرنامج.

وفيما يتعلق بشراء برنامج Kaspersky الذي يهدف إلى خدمة العملاء الأفراد من طريق آخر بخلاف الإنترنت، لن يمكن إعادة البرنامج أو استبداله إلا في حالة وجود شروط مناقضة نص عليها الشريك الذي يبيع هذا المنتج. وفي هذه الحالة لن تلتزم Kaspersky LAB بالمواد التي ينص عليها الشريك.

يقتصر حق الرد واسترداد القيمة على المشتري الأصلي.

تعتبر جميع الإشارات إلى كلمة "البرنامج" في هذه الاتفاقية شاملة شفرة تفعيل البرنامج التي ستمنحك إياها شركة Kaspersky Lab كجزء من برنامج مكافحة الفيروسات من Kaspersky.

1. منح الترخيص. تمنحك Kaspersky Lab بموجب هذه الاتفاقية حقاً عاماً يحظر منحه إلى شخص آخر لاستخدام البرنامج والوثائق المصاحبة، المشار إليها باسم ("الوثائق")، طوال مدة هذه الاتفاقية فقط لأغراض أعمالك التجارية الداخلية، وفقا لسداد رسوم الترخيص المعمول بها، ووفقاً لبنود وشروط هذه الاتفاقية. يجوز لك تثبيت نسخةٍ واحدةٍ من البرنامج على جهاز كمبيوتر واحد.

1.1 الاستخدام. إذا اشتريت البرنامج على وسيط مادي، يحق لك استخدامه لحماية العدد المذكور على العبوة من أجهزة الكمبيوتر. إذا اشتريت البرنامج عن طريق الإنترنت، يحق لك استخدامه لحماية العدد الذي طلبته من أجهزة الكمبيوتر عند شراء البرنامج.

1.1.1 يكون البرنامج "قيد الاستخدام" على جهاز كمبيوتر عندما يتم تحميله إلى الذاكرة المؤقتة (أي ذاكرة الوصول العشوائي) أو تثبيته على الذاكرة الدائمة لذلك الكمبيوتر (مثل القرص الثابت أو القرص المدمج أو غير ذلك من أجهزة التخزين). لا يخول لك هذا الترخيص إلا بإنشاء نُسخ احتياطية من البرنامج حسبما يكون ضرورياً

للاستخدام القانوني له بحيث لا يتعدى ذلك أغراض النسخ الاحتياطي وشريطة أن تحتوي جميع تلك النُسخ على إشعارات ملكية البرنامج. يتعين عليك أن تحتفظ بسجلات لعدد جميع نُسخ البرنامج ووثائقه ومكانها واتخاذ جميع الاحتياطات المعقولة لحماية البرنامج من النسخ أو الاستخدام غير المصرح بهما.

1.1.2 يحمي البرنامج جهاز الكمبيوتر من الفيروسات التي توجد توقيعاتها في قاعدة بيانات التوقيعات الخطرة، وهي متاحة على خوادم تحديث Kaspersky Lab.

1.1.3 في حالة بيع جهاز الكمبيوتر المثبت عليه البرنامج، يتعين عليك ضمان حذف جميع نُسخ البرنامج مسبقاً.

1.1.4 يحظر عليك إلغاء ترجمة البرنامج (تحويل برنامج من لغة الآلة إلى لغة البرمجة) أو استكشاف نظام عمله أو إلغاء تجميعه (تحويل برنامج من لغة الآلة إلى لغة رمزية)، أو بطريقة أخرى تحويل أي جزء منه إلى نموذج يصلح قراءته بشرياً، أو السماح لأي طرف ثالث بفعل أي مما سبق. سيتم توفير معلومات الواجهة اللازمة لتحقيق قابلية التشغيل المتبادل للبرنامج مع برامج الكمبيوتر المنشأة بشكل مستقل بواسطة Kaspersky Lab عند طلبها لدى سداد التكاليف والمصروفات المعقولة للحصول على تلك المعلومات والتزويد بها. وفي حالة إخطارك من قبل Kaspersky Lab بأنها لا تعتزم إتاحة مثل تلك المعلومات لأي سبب كان، بما في ذلك (على سبيل المثال لا الحصر) التكاليف، فإنه يُسمح لك باتخاذ تلك الخطوات لتحقيق قابلية التشغيل المتبادل، شريطة أن يكون استخدامك للترجمة العكسية أو إلغاء ترجمة البرنامج فقط بالقدر الذي يسمح به القانون.

1.1.5 يتعين عليك عدم تصحيح أخطاء البرنامج، أو تعديله أو مواءمته أو ترجمته أو غير ذلك من أشكال التغيير، وكذلك عدم إنشاء أعمال مشتقة من البرنامج ولا السماح لأي طرف ثالث بالنسخ (باستثناء ما هو مسموح به صراحة في هذه الاتفاقية).

1.1.6 يتعين عليك عدم تأجير البرنامج بصورة دائمة أو لفترة محدودة أو إقراضه إلى أي شخص، وعدم نقله إلى أي شخص آخر أو منح حقوق الترخيص إلى أي طرف ثالث.

1.1.7 يتعين عليك عدم تقديم رمز التفعيل أو ملف مفتاح الترخيص إلى أطراف ثالثة أو السماح بوصول أطراف ثالثة إلى رمز التفعيل أو مفتاح الترخيص. يعتبر كل من رمز التفعيل ومفتاح الترخيص بيانات سرية.

1.1.8 يحق لشركة Kaspersky Lab مطالبتك بتثبيت أحدث إصدار من البرنامج (أحدث إصدار وأحدث حزمة خدمات صيانة).

1.1.9 يتعين عليك عدم استخدام هذا البرنامج بالأدوات التلقائية أو شبه التلقائية أو اليدوية المصممة لإنشاء توقيعات الفيروس، أو أنظمة اكتشاف الفيروس، أو أي بيانات أو رموز أخرى تخص اكتشاف الرموز أو البيانات الخبيثة.

1.1.10 إن شركة Kaspersky Lab، وفقاً لموافقتك المؤكدة صراحة في بيان يفيد بذلك، يحق لها أن تجمع معلومات بشأن التهديدات المحتملة ونقاط الاختراق من جهاز الكمبيوتر الخاص بك.. وعلى ذلك فإن المعلومات المجمعة تستخدم بصورة عامة لا لغرض سوى تحسين منتجات Kaspersky Lab.

2. الدعم [1].

---

[1] عند استخدام النسخة التجريبية من البرنامج، لن يحق لك الحصول على الدعم الفني المحدد في المادة 2 من اتفاقية ترخيص المستخدم النهائي هذه وكذلك لا يحق لك بيع النسخة الخاصة بك إلى أطراف أخرى.

وإنما يكون لك الحق في استخدام البرنامج للأغراض التجريبية لفترة من الوقت تحدد في ملف مفتاح الترخيص تبدأ من لحظة التفعيل (يمكن رؤية هذه الفترة في نافذة الخدمة الخاصة بواجهة المستخدم الرسومية للبرنامج).

(ط) تقدم لك Kaspersky Lab خدمات الدعم (والمشار إليها فيما بعد بـ "خدمات الدعم") كما هو محدد أدناه لفترة محددة في ملف مفتاح الترخيص (فترة الخدمة) كما هو مبين في نافذة "الخدمة"، ابتداءً من وقت التفعيل عند:

(أ) سداد تكلفة الدعم الخاصة بها في ذلك الوقت؛ و

(ب) نجاح إكمال طلب الاشتراك في خدمات الدعم المقدم إليك مع هذه الاتفاقية أو المتاح على موقع شركة Kaspersky Lab على الويب، والذي سيطلب منك إدخال رمز التفعيل الذي تقدمه أيضا شركة Kaspersky Lab مع هذه الاتفاقية. يكون لشركة Kaspersky Lab السلطة التقديرية المطلقة في تقرير ما إذا كنت قد استوفيت هذا الشرط المطلوب لتقديم خدمات الدعم أم لا.

تصبح خدمات الدعم متاحة بعد تفعيل البرنامج. لخدمة الدعم الفني في شركة Kaspersky Lab الحق في أن تطلب منك تسجيلاً إضافياً لمنح المعرف المعرف الخاص بتقديم خدمة الدعم.

لا تقوم خدمة الدعم الفني بتقديم المساعدة إلا في تفعيل البرنامج وتسجيل المستخدم النهائي إلى أن يتم تفعيل البرنامج و/أو الحصول على معرف المستخدم النهائي (معرف العميل).

(2) سوف تنتهي خدمات الدعم ما لم يتم تجديدها سنوياً بسداد رسم الدعم السنوي الساري في ذلك الوقت وبعد نجاح إكمال طلب الاشتراك في خدمات الدعم مرة أخرى.

(3) تعني "خدمات الدعم":

(أ) التحديثات المنتظمة لقاعدة بيانات مكافحة الفيروسات؛ و

(ب) التحديثات المجانية للبرامج، بما في ذلك ترقيات الإصدار؛ و

(ج) الدعم الفني عبر الإنترنت وخط تليفوني ساخن يوفره البائع و/أو الموزع؛ و

(د) اكتشاف الفيروسات وتطهير التحديثات خلال 24 ساعة.

(4) لا تُقدم خدمات الدعم إلا في حالة امتلاكك لأحدث إصدار من البرنامج (بما في ذلك حزم خدمات الصيانة) كما هو متاح على الموقع الرسمي لشركة Kaspersky Lab (www.kaspersky.com) وتثبيته على الكمبيوتر الخاص بك.

3. حقوق الملكية. eP3 البرنامج محمي بموجب قوانين حقوق التأليف والنشر. تملك وتحتفظ شركة Kaspersky Lab وموزعوها بجميع الحقوق وحقوق الملكية والمصالح في البرنامج بما في ذلك جميع حقوق التأليف والنشر وبراءات الاختراع والعلامات التجارية وغيرها من حقوق الملكية في ذلك. لا يكون من شأن حيازتك للبرنامج أو تثبيته أو استخدامه أن ينقل إليك أي حق من حقوق الملكية الفكرية للبرنامج ولن تكتسب أي حقوق في البرنامج فيما عدا ما هو وارد صراحة في هذه الاتفاقية.

4. السرية. توافق على أن البرنامج والوثائق، بما في ذلك التصميم والبنية المحددين للبرامج الفردية، يشكلان معلومات سرية تمتلكها شركة Kaspersky Lab. ينبغي عليك عدم الإفصاح عن تلك المعلومات السرية أو تقديمها أو إتاحتها بخلاف ذلك لأي طرف ثالث دون موافقة كتابية مسبقة من Kaspersky Lab. يتعين عليك

تطبيق إجراءات الأمان المعقولة لحماية تلك المعلومات السرية غير أنه يتعين عليك، دون الاقتصار على ما سبق ذكره، بذل أفضل الجهود للمحافظة على حماية رمز التفعيل.

5. الضمان المحدود.

(ط) تضمن Kaspersky Lab كفاءة عمل البرنامج المشترى على وسيط مادي لمدة ستة (6) أشهر اعتباراً من أول تحميل أو تثبيت للبرنامج وفقاً لكفاءة التشغيل المبينة في الوثائق عند تشغيله كما ينبغي وبالطريقة المحددة في الوثائق.

(2) تقبل المسؤولية كاملة عن اختيارك لهذا البرنامج للوفاء بمتطلباتك. ولا تضمن Kaspersky Lab أن يكون البرنامج و/أو الوثائق مناسبين لتلك المتطلبات ولا عدم توقف البرنامج أو عدم حدوث أخطاء به عند القيام بأي نوع من أنواع الاستخدام للبرنامج.

(3) لا تضمن Kaspersky Lab أن هذا البرنامج يتعرف على كافة الفيروسات المعروفة، ولا أنه لن يقدم تقارير خاطئة من حين لآخر عن وجود فيروس باسم غير مصاب بهذا الفيروس.

(4) يكون سبيل التعويض الوحيد لك والمسؤولية الكاملة على Kaspersky Lab مقابل انتهاك الضمان الوارد في الفقرة (1) تبعاً لاختيار Kaspersky Lab إما بإصلاح البرنامج أو استبداله أو رد قيمته إذا تم إبلاغ ذلك الانتهاك إليها أو إلى من تعينه أثناء فترة الضمان. يتعين عليك تقديم جميع المعلومات حسبما يكون ضرورياً بشكلٍ معقولٍ لمساعدة المورد في التقرير بشأن العنصر المعطوب.

(5) لا يُنفذ الضمان الوارد في الفقرة (1) إذا قمت بـ (أ) إجراء أي تعديلات للبرنامج أو تسببت في ذلك دون موافقة Kaspersky Lab، (ب) استخدام البرنامج بطريقة تخالف الغرض الذي أنشئ له البرنامج، أو (ج) استخدام البرنامج بطريقة تخالف المسموح به بموجب هذه الاتفاقية.

(6) تحل الضمانات والشروط المنصوص عليها في هذه الاتفاقية محل جميع الشروط أو الضمانات الأخرى أو البنود الأخرى المتعلقة بتوريد البرنامج أو ما يفيد هذا التوريد، أو الإخفاق في التوريد أو تأخره، أو الوثائق التي يمكن لغرض هذه الفقرة أن (6) تكون سارية بين شركة Kaspersky Lab وبينك، أو التي تكون مفهومةً ضمناً أو متضمنةً بخلاف ذلك في هذه الاتفاقية أو أي عقد إضافي، سواءً أكان ذلك بموجب التشريع أو القانون العام أو بخلاف ذلك، وتكون جميعها مستثناة بموجب هذه الاتفاقية (بما في ذلك على سبيل المثال لا الحصر الشروط أو الضمانات أو البنود الأخرى الضمنية فيما يتعلق بالجودة المرضية وملائمة الغرض أو فيما يتعلق باستخدام المهارة والعناية المعقولتين).

6. حدود المسؤولية.

(ط) لا يستثني أي مما ورد في هذه الاتفاقية أو يحد من مسؤولية Kaspersky Lab عن: (أ) الاحتيال؛ أو (ب) الوفاة أو الإصابة الشخصية الناشئة عن خرقها لواجب العناية تبعاً للقانون العام أو أي خرق - ناشئ عن الإهمال - لأي من بنود هذه الاتفاقية؛ أو (ج) أية مسؤولية أخرى لا يمكن استثناؤها بموجب القانون.

(2) طبقاً للفقرة (1) أعلاه، لا تتحمل شركة Kaspersky Lab أية مسؤولية (سواء فيما يتعلق بالعقد أو الضرر أو التعويض أو غير ذلك) عن أي من الخسائر أو الأضرار التالية (سواءً أكانت تلك الخسائر أو الأضرار متنبأ بها أو متوقعة أو معروفة أو غير ذلك):

(أ) خسارة الإيراد؛ أو

(ب) خسارة الأرباح الفعلية أو المتوقعة (بما في ذلك خسارة أرباح العقود)؛ أو

(ج) خسارة الانتفاع بالأموال؛ أو

(د) خسارة المدخرات المتوقعة؛ أو

(هـ) خسارة الأعمال؛ أو

(و) فوات الفرص؛ أو

(ز) فقدان الشهرة؛ أو

(ح) فقدان السمعة؛ أو

(ط) فقدان البيانات أو تلفها أو دمارها؛ أو

(ي) أية خسارة أو تلف غير مباشرين أو تبعيين أيا كان سببهما (بما في ذلك، لتجنب الشك، متى كانت تلك الخسارة أو التلف من النوع المحدد في الفقرات من (2)(أ) إلى (2)(ط).

(3) طبقاً للفقرة (1) أعلاه، لا تتجاوز مسؤولية Kaspersky Lab (سواء فيما يتعلق بالعقد أو الضرر أو التعويض أو غير ذلك) الناشئة عن توريد البرنامج أو فيما يتعلق به بأي حالٍ من الأحوال مبلغاً يعادل المبلغ الذي قمت بدفعه لشراء البرنامج.

7. تحتوي هذه الاتفاقية على الاتفاق الكامل بين الأطراف فيما يتعلق بموضوعها وتحل محل أي من وجميع الاتفاقات والتعهدات والوعود السابقة بينك وبين Kaspersky Lab سواءً أكانت شفهية أم كتابية، والتي قد أعطيت صراحة أو فُهمت ضمناً من أي مستند كتابي أو ذكرت في مفاوضات بيننا أو بين وكلائنا قبل هذه الاتفاقية ويتوقف سريان جميع الاتفاقيات السابقة بين الأطراف ذات الصلة بالأمور المذكورة آنفاً اعتباراً من تاريخ السريان.